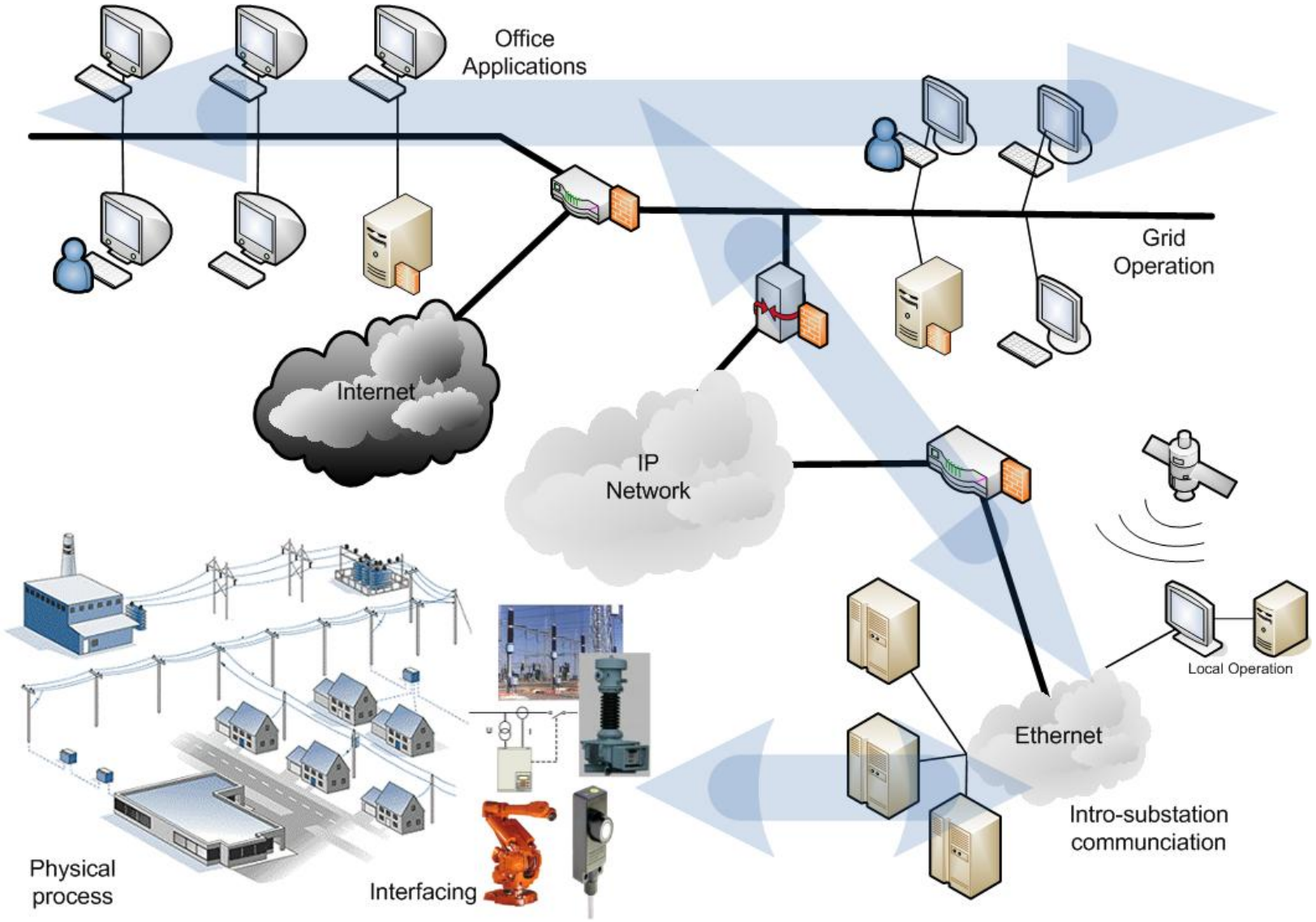
ROYAL INSTITUTE
OF TECHNOLOGY

Communication Systems I

ROYAL INSTITUTE OF TECHNOLOGY

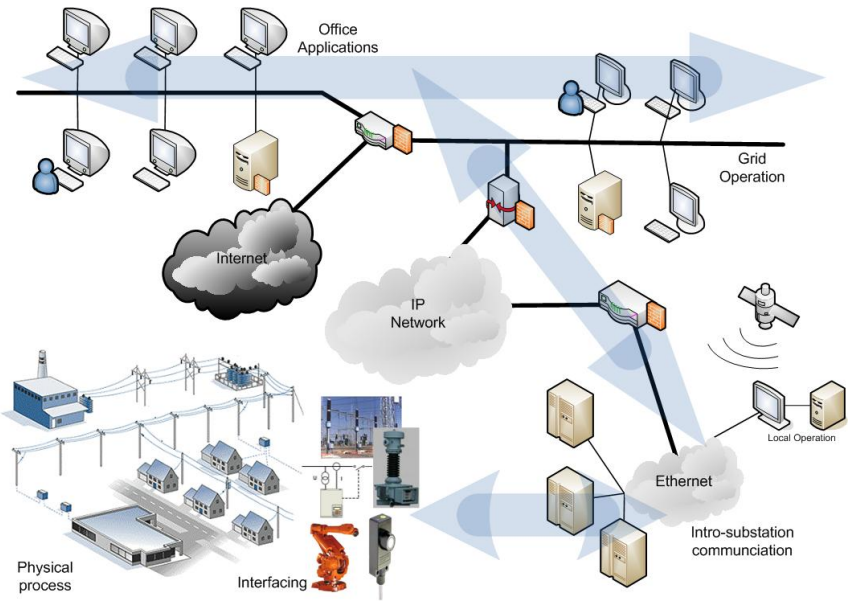
Course Map



ROYAL INSTITUTE OF TECHNOLOGY

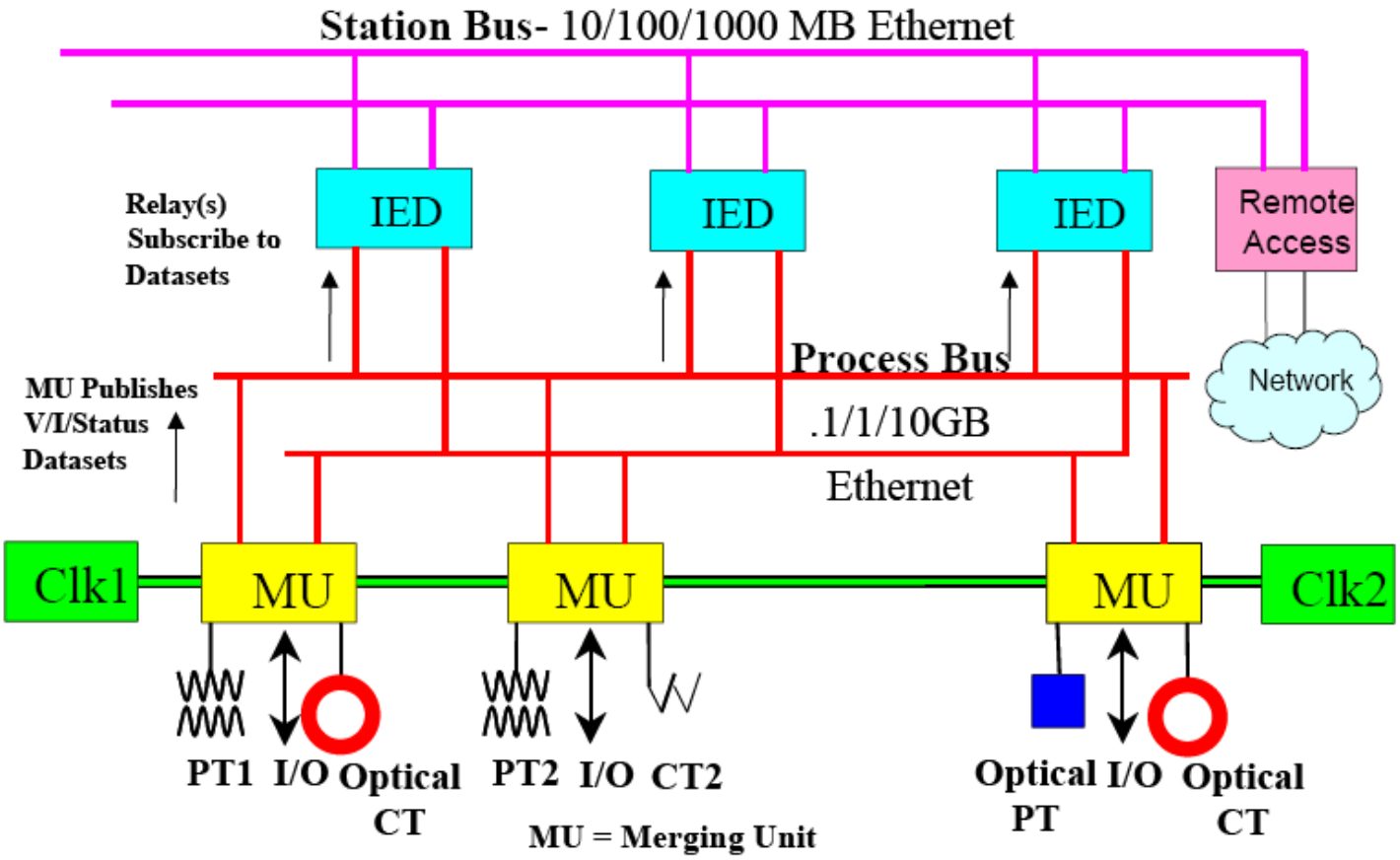
Contents

- Recap of the networks we've seen so far
- Basics of protocols – HTTP example
- The OSI model
- Packet and Circuit switching
- Physical media
- What to expect next



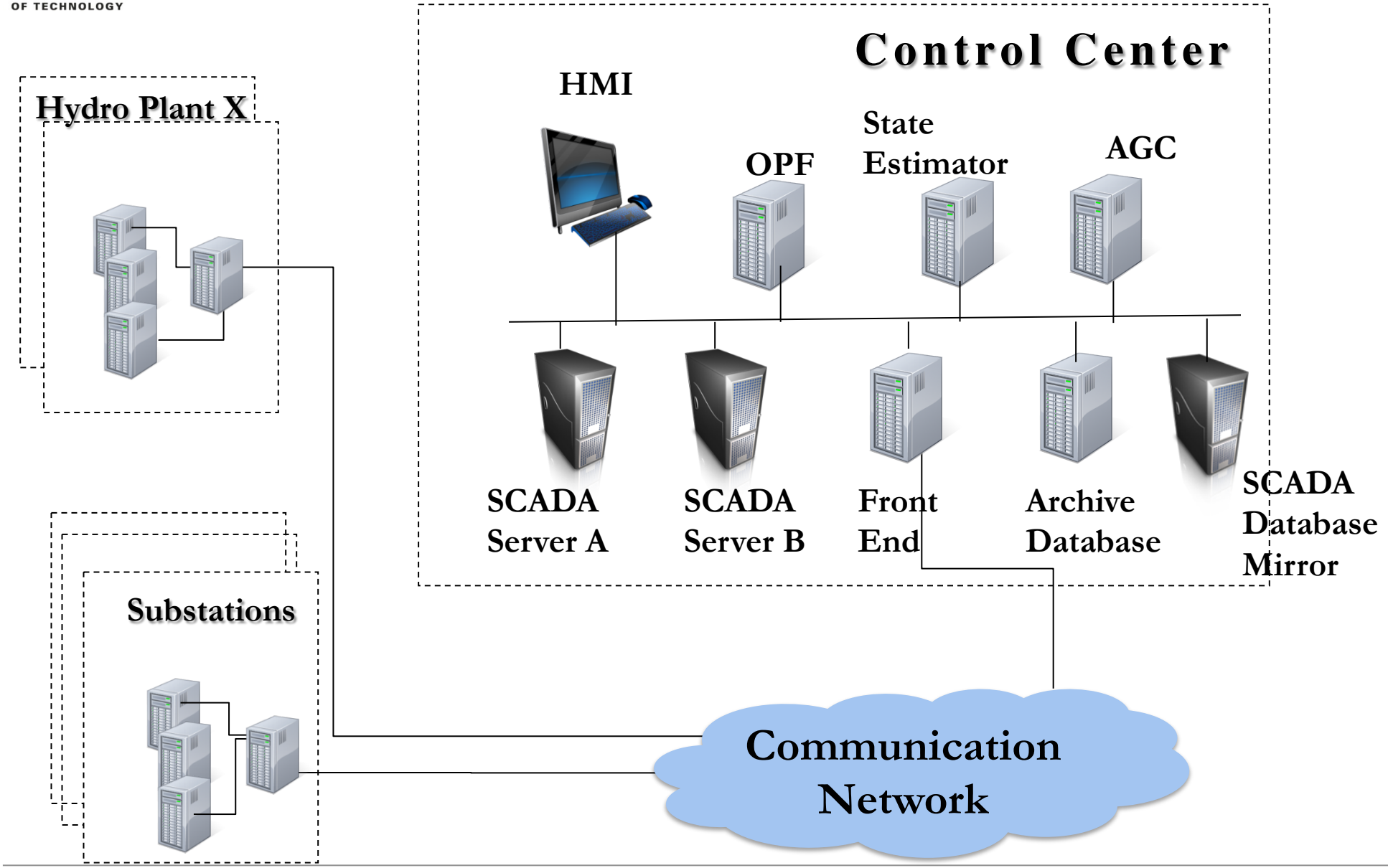
Recap

Substation Networks



Recap

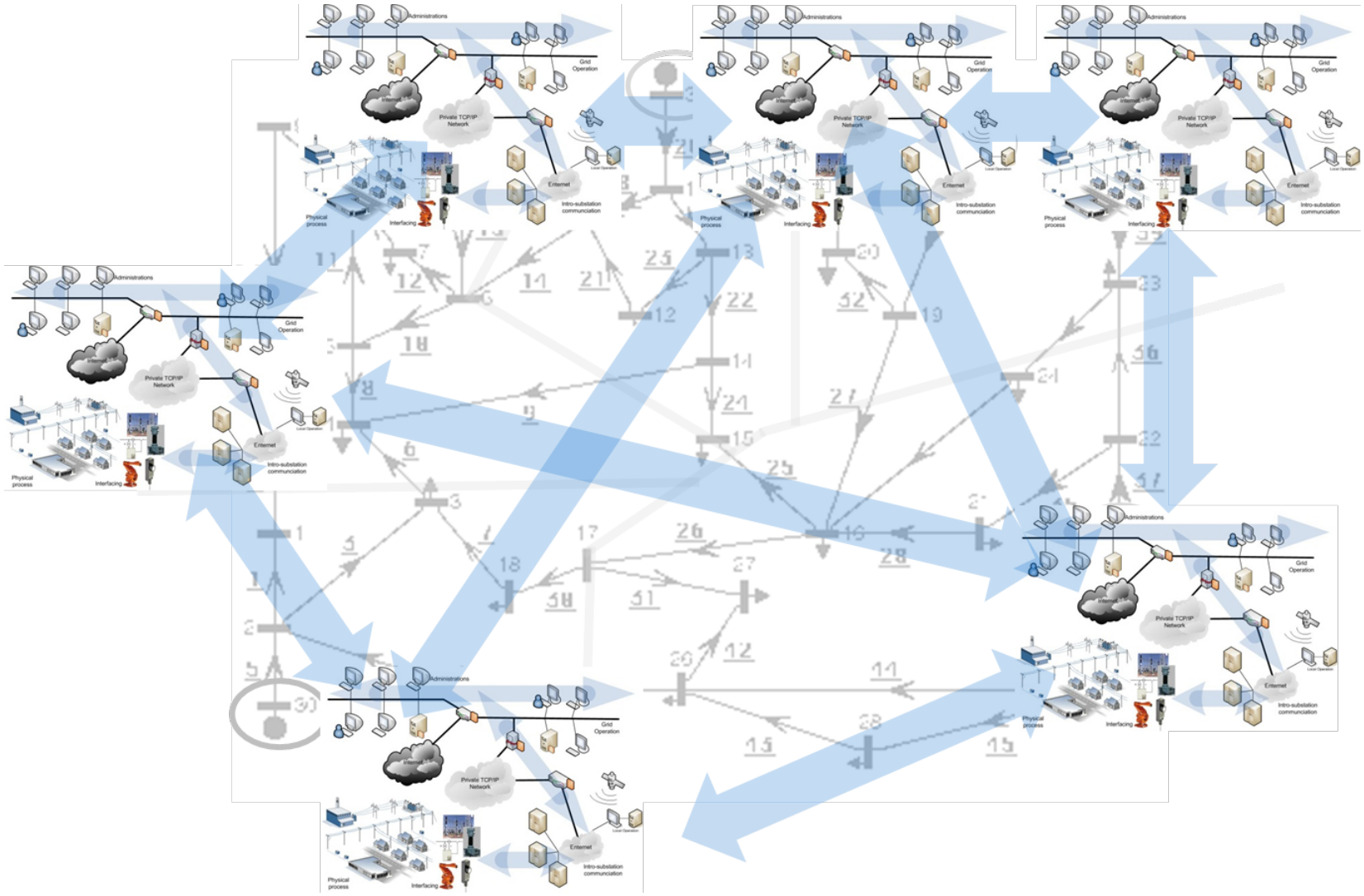
SCADA Networks



ROYAL INSTITUTE OF TECHNOLOGY

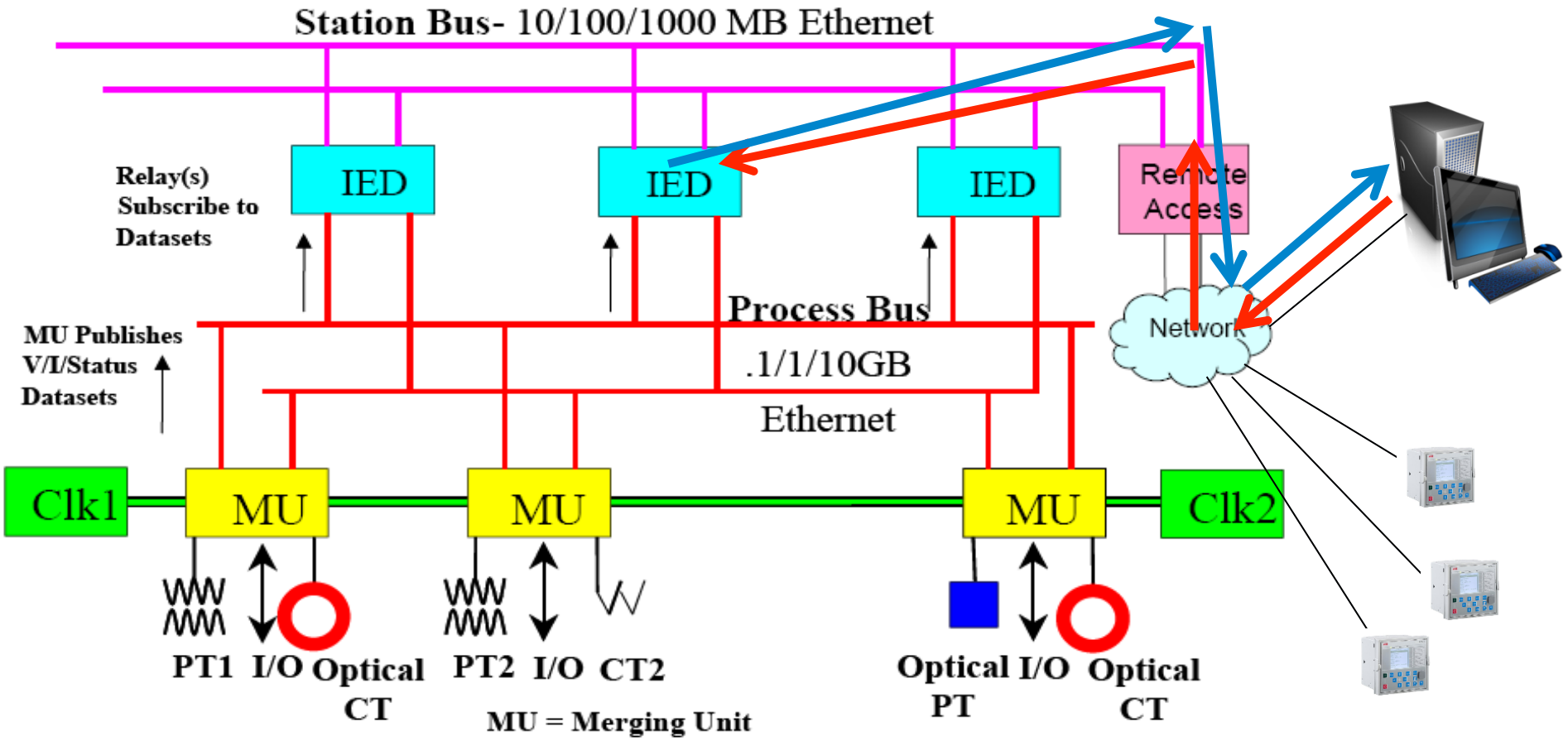
Recap

SCADA Networks



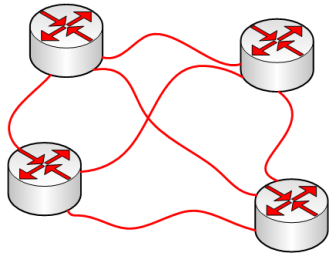
Recap

Modern substation



ROYAL INSTITUTE OF TECHNOLOGY

Protocol Basics

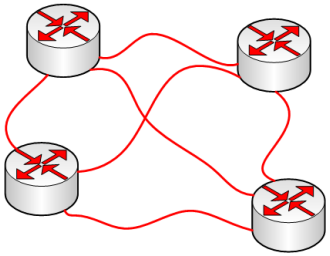


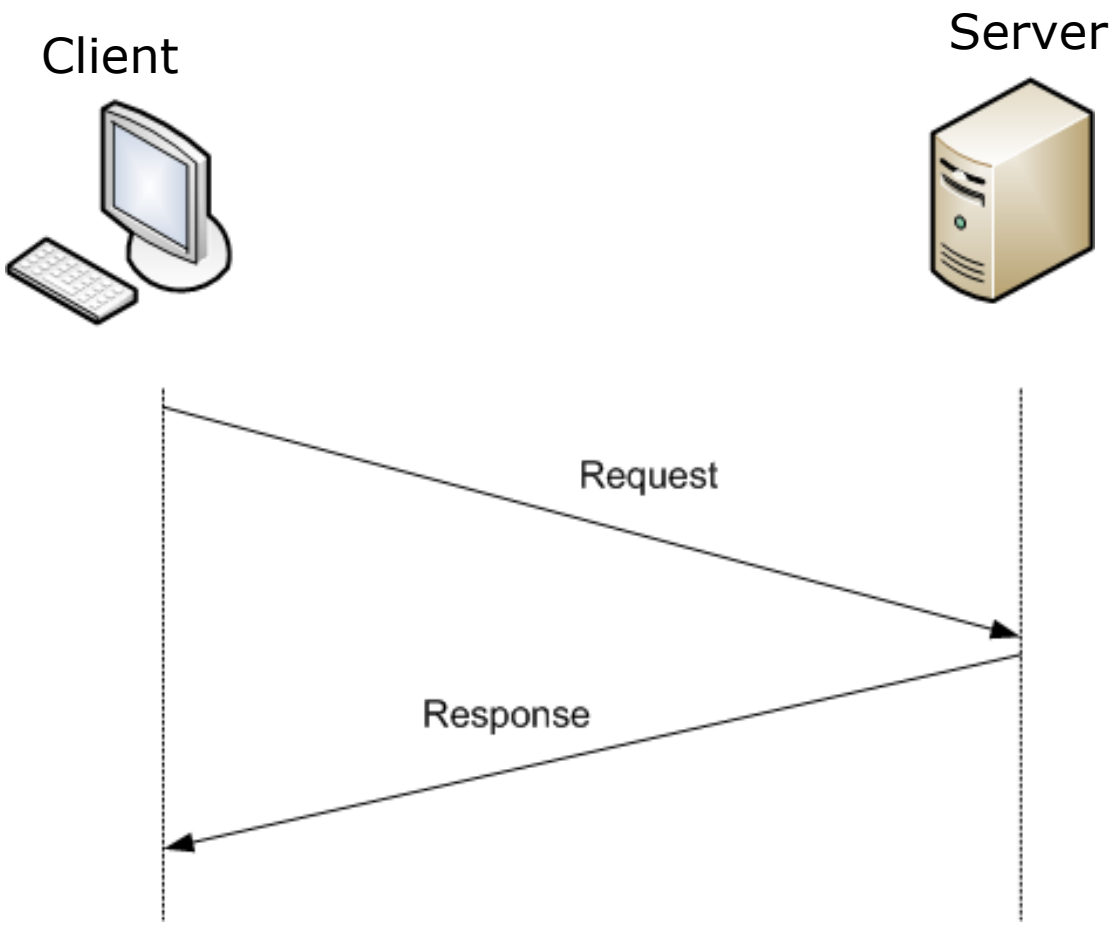
- Basic Protocol
- HTTP protocol – example
- Wireshark
- Some observations from the example

ROYAL INSTITUTE OF TECHNOLOGY

Protocol Basics

Basic protocol

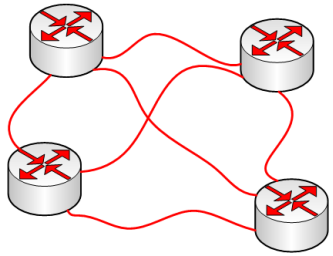




ROYAL INSTITUTE OF TECHNOLOGY

Protocol Basics

Basic protocol

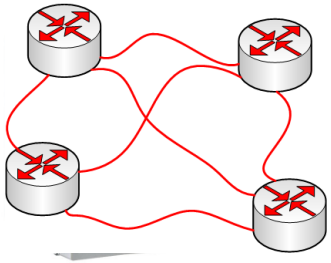


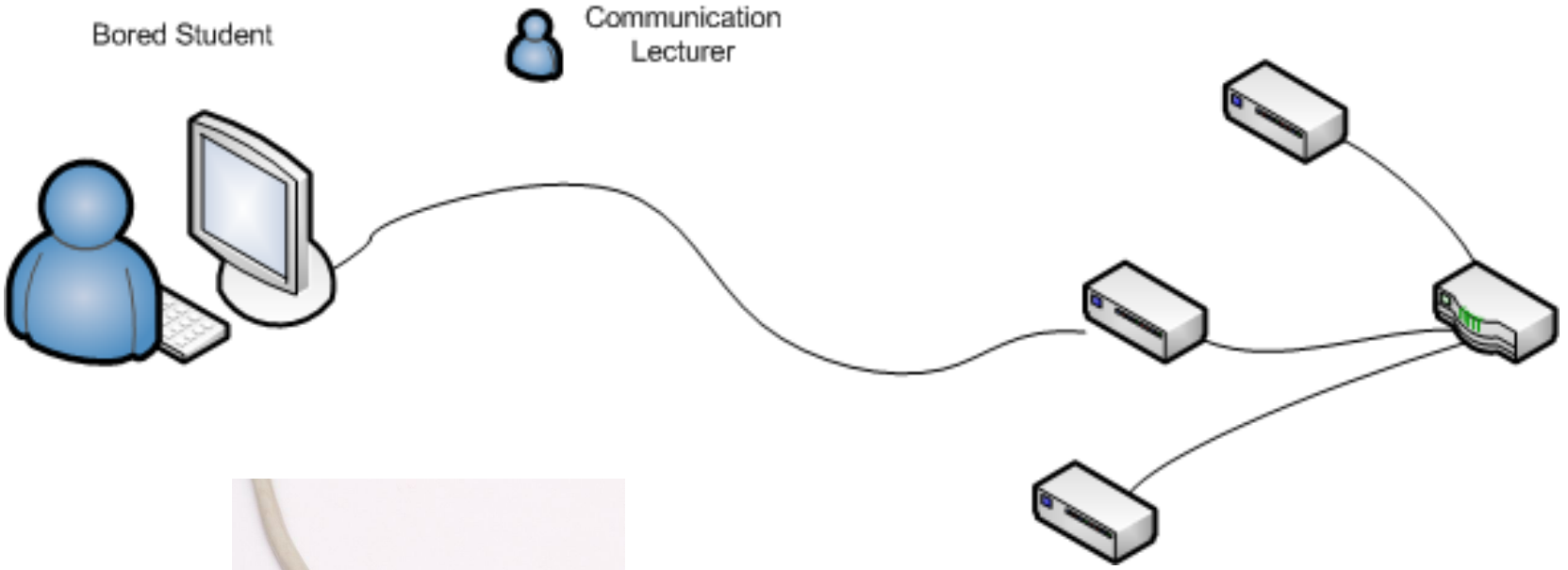
We use these continuously!

ROYAL INSTITUTE OF TECHNOLOGY

Protocol Basics

HTTP protocol

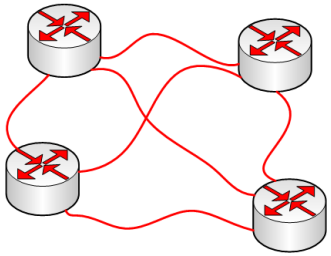


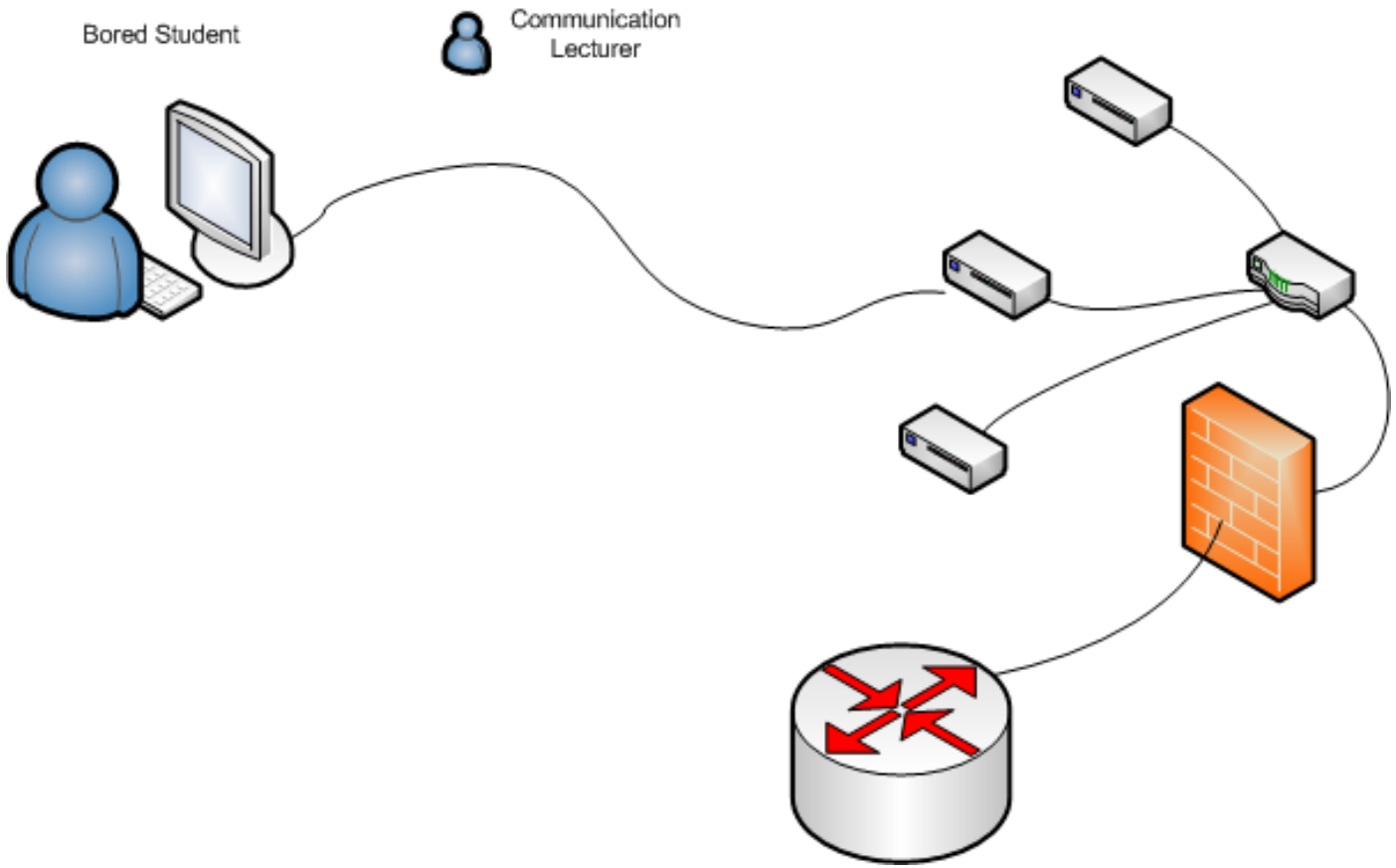


ROYAL INSTITUTE OF TECHNOLOGY

Protocol Basics

HTTP protocol

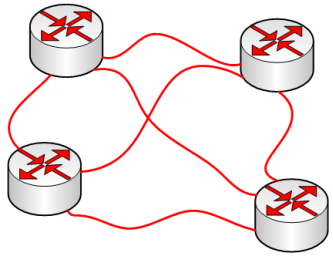


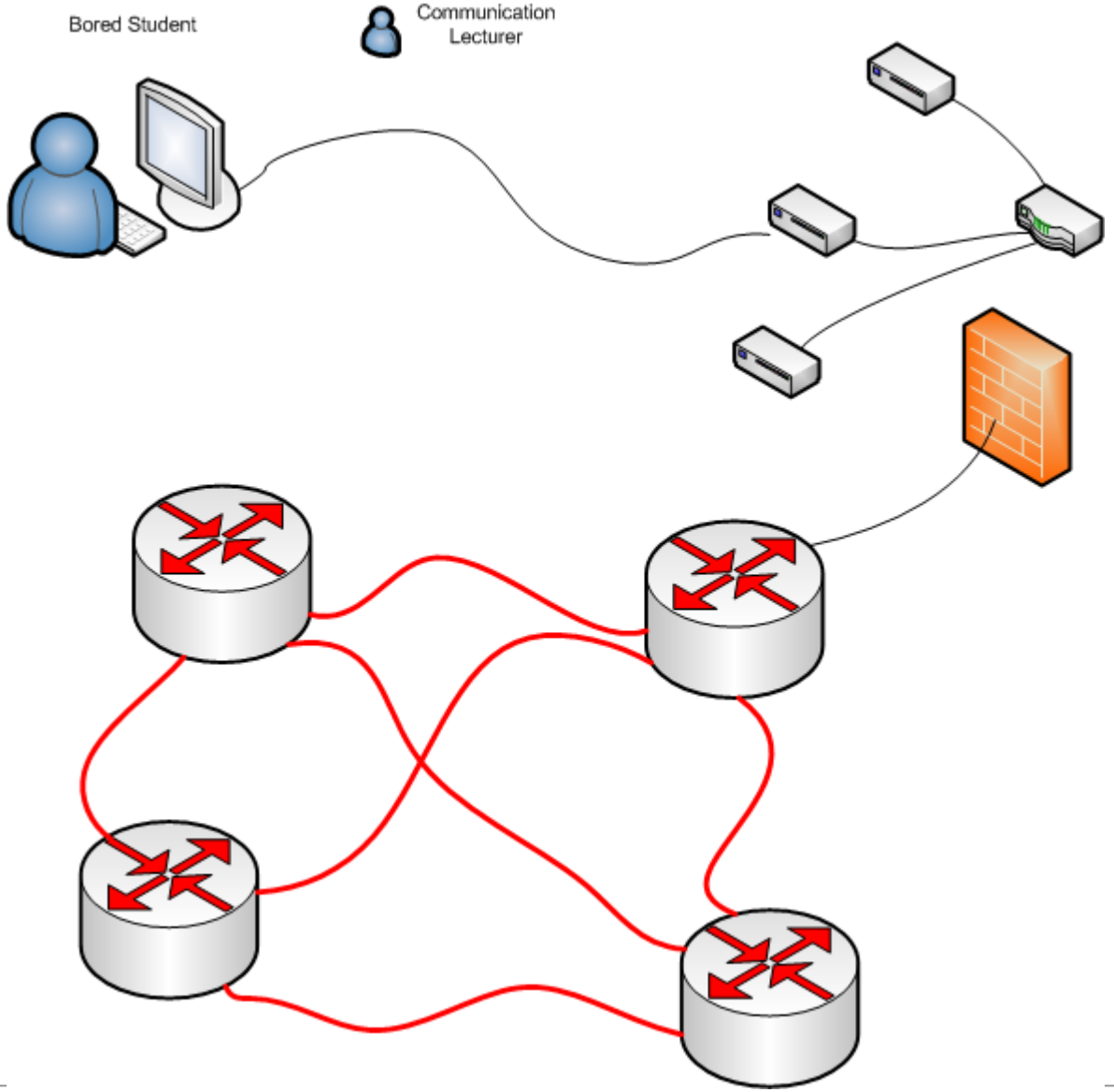


ROYAL INSTITUTE OF TECHNOLOGY

Protocol Basics

HTTP protocol

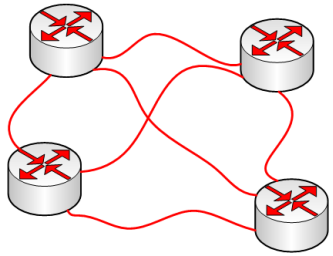


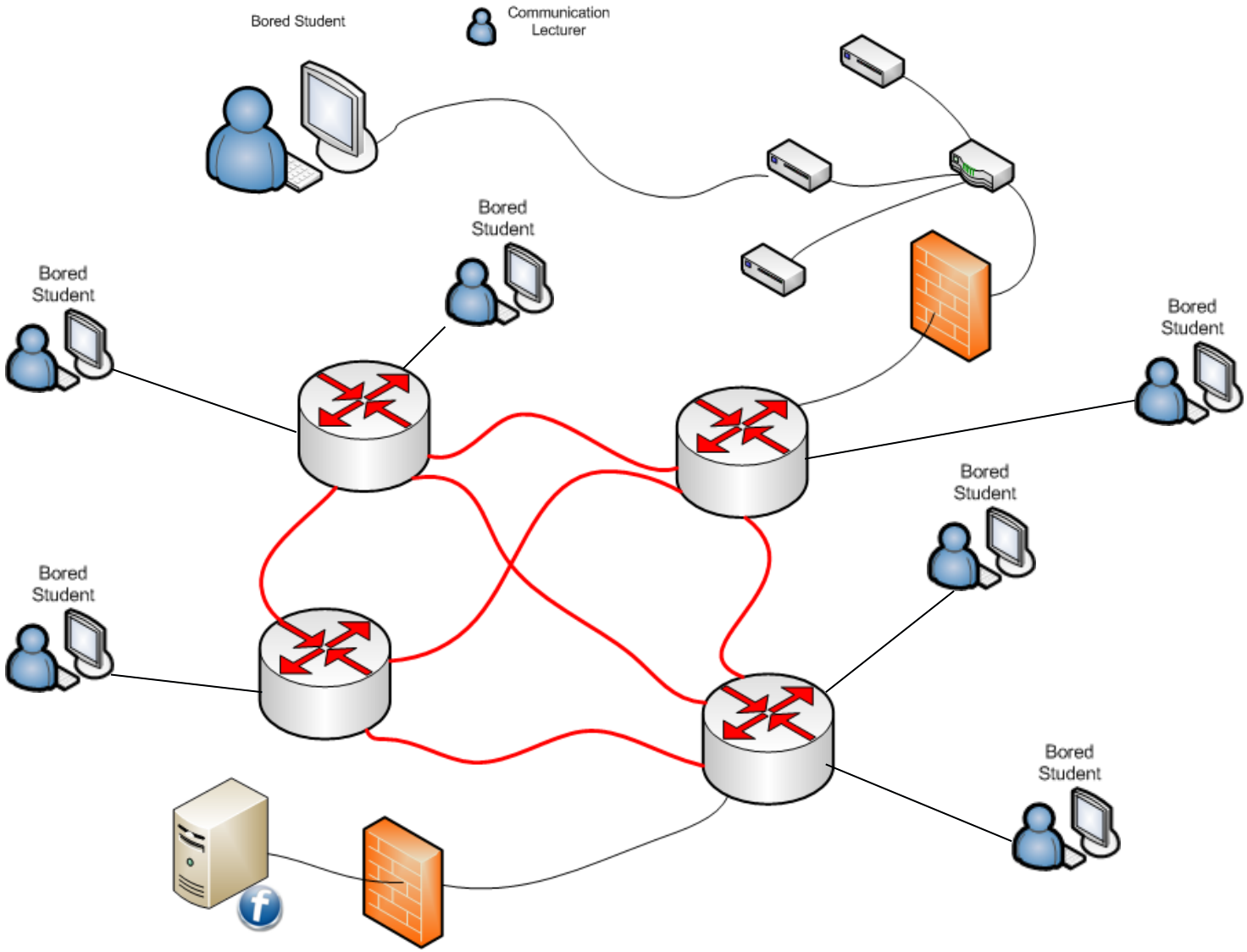


ROYAL INSTITUTE OF TECHNOLOGY

Protocol Basics

HTTP protocol

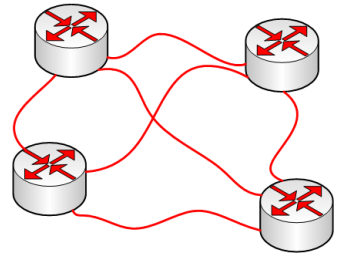




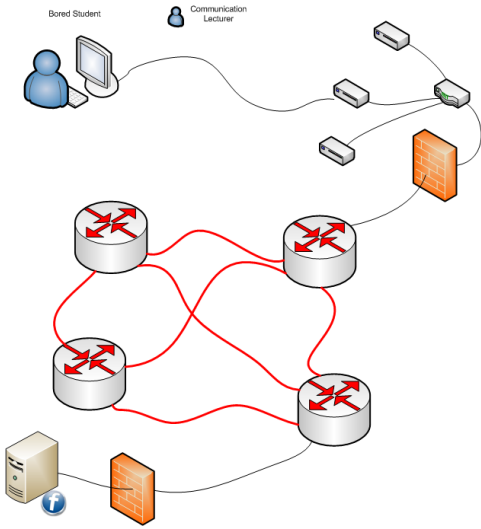
ROYAL INSTITUTE OF TECHNOLOGY

Protocol Basics

HTTP protocol



- What program/application does the student use to access the service?
  - An application that implements the protocol - browser
- How is the desired service identified?
  - URL - Uniform Resource Locator
- How does the student request information?
  - HTTP GET message
- How does the student host know where to send the request?
  - IP address
  - Routing table
- What carries the message to the service provider?
  - Network infrastructure – LAN -> Internet (WAN)



ROYAL INSTITUTE OF TECHNOLOGY

Application
Transport
Network
Data Link
Physical

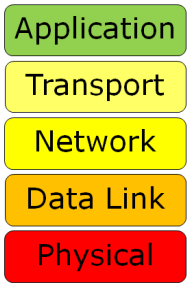
The OSI model

- Layering
- OSI model – long version
- OSI model – short version
- Headers
- OSI layers
  - Application layer
  - Transport layer
  - Network layer
  - Data link layer
  - Physical layer
- Transision between layers

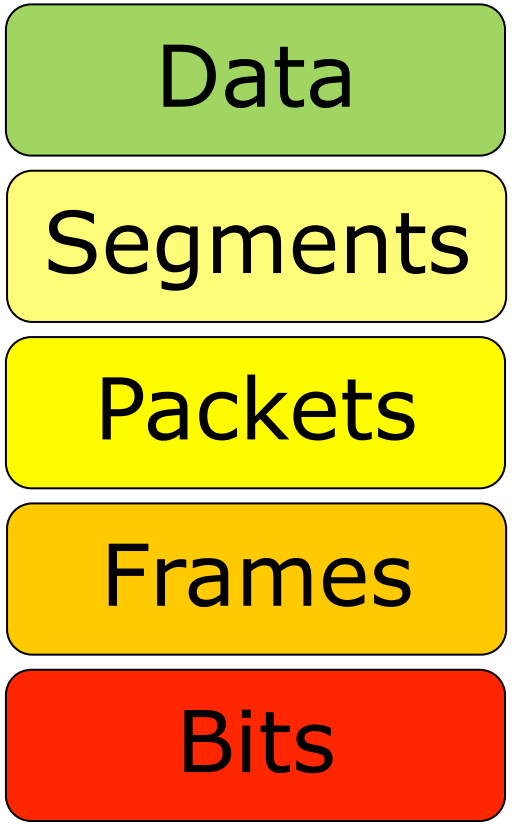
ROYAL INSTITUTE OF TECHNOLOGY

The OSI model

Layering



- Units of high-level **protocol data** eg. HTML
- Data is **segmented**, sometimes into streams (TCP) or “datagrams” (UDP)
- Each segment is **packaged** to be sent across a network.
- The package is enclosed in a **frame** to be sent on the **link** eg. Ethernet
- The frame is transmitted as a string of **binary bits** on the physical media eg. UTP



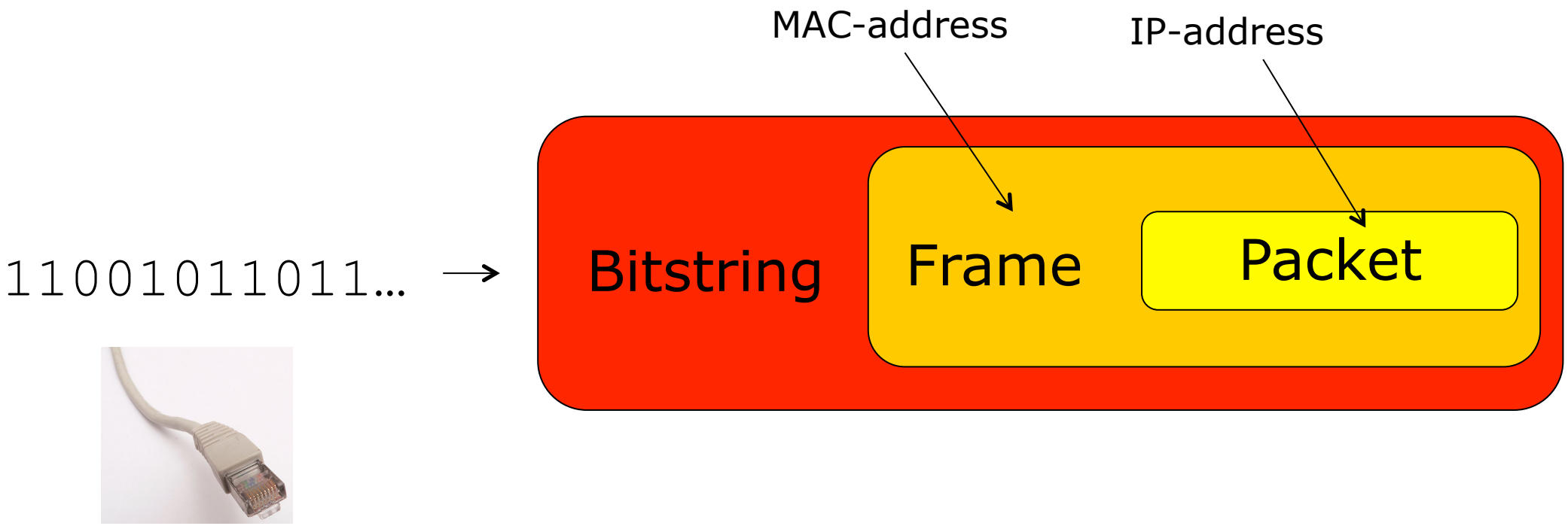
ROYAL INSTITUTE OF TECHNOLOGY

The OSI model

Layering

Application
Transport
Network
Data Link
Physical

- Each layer encapsulates the container of the layer above
- Identification and addressing information for each layer

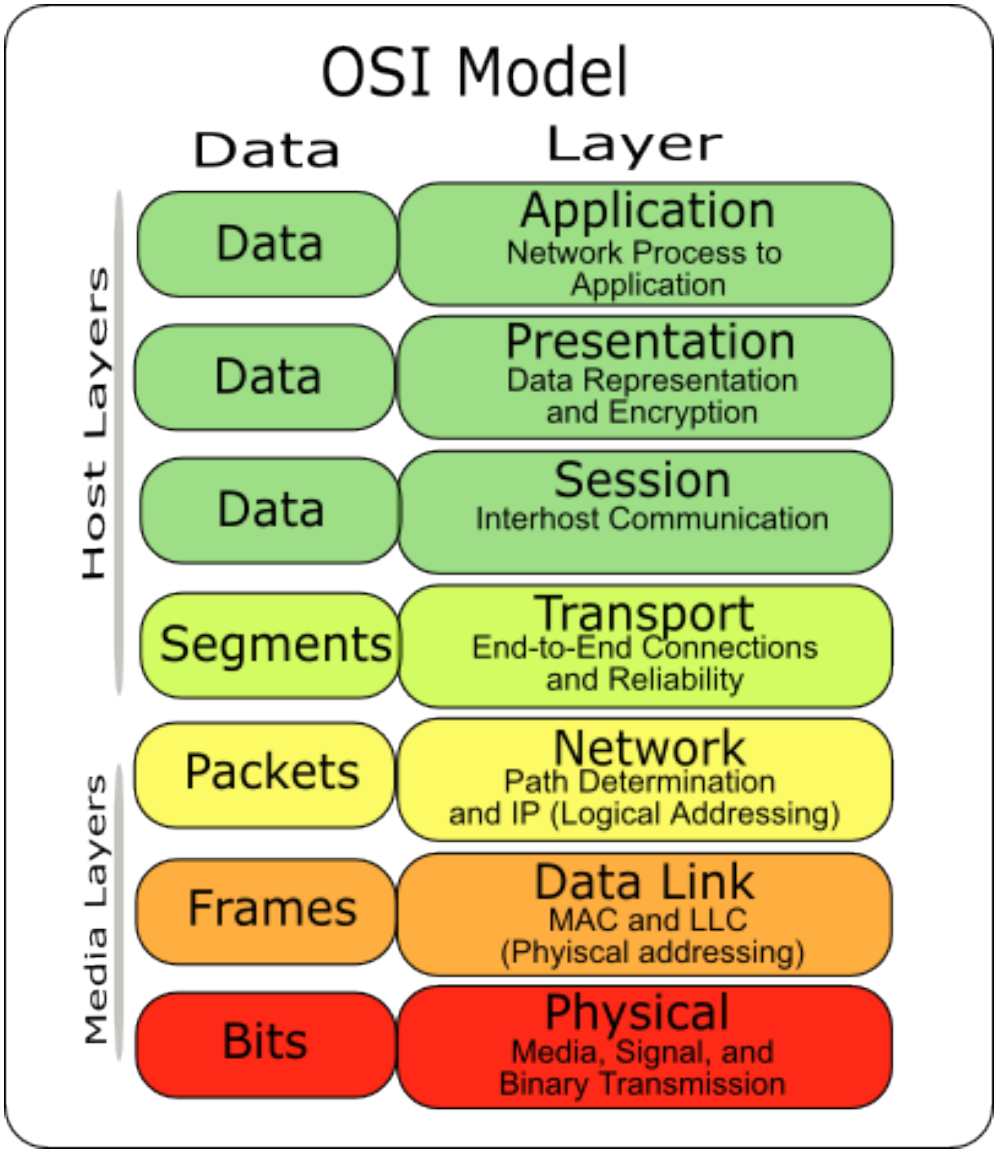


ROYAL INSTITUTE OF TECHNOLOGY

The OSI model

Long version

Application
Transport
Network
Data Link
Physical



ROYAL INSTITUTE OF TECHNOLOGY

The OSI model

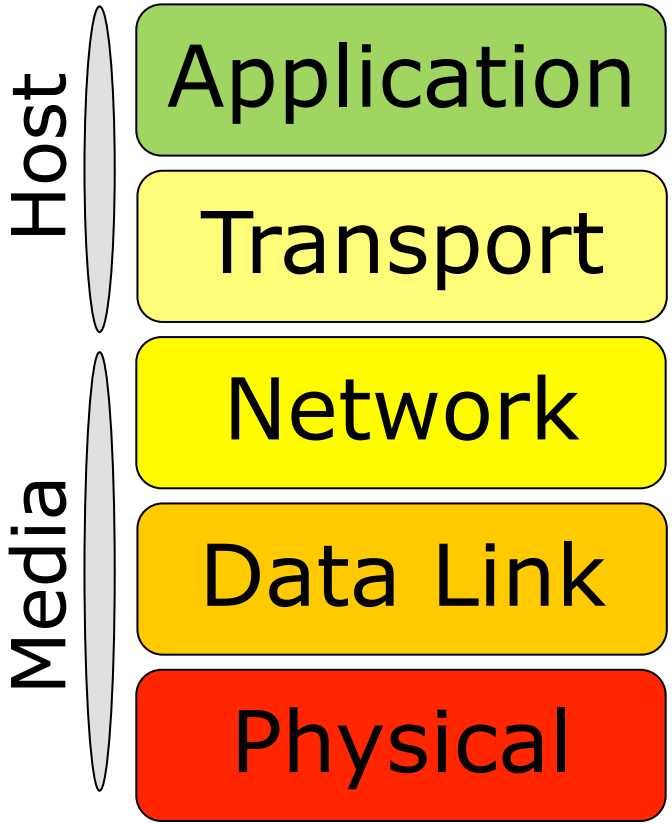
Short version

Application
Transport
Network
Data Link
Physical

- Session and Presentation layers viewed as application-internal and are not modeled

- Lower 3 layers part of network infrastructure.
  - More generalized

- Top layers mainly associated with host-host applications.
  - Application specific eg. HTTP



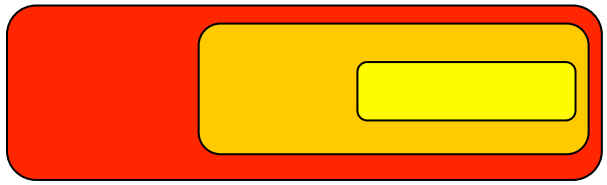
ROYAL INSTITUTE OF TECHNOLOGY

The OSI model

Headers

Application
Transport
Network
Data Link
Physical

- Additional information for each OSI layer:
  - Contained in **headers:**
    - **Transport**
      - Source/destination port
      - …
    - **Network**
      - Source/destination IP address
      - …
    - **Data Link**
      - Source/destination MAC address
      - …



Application

Transport

Network

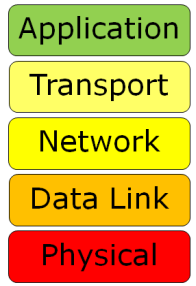
Data Link

Physical

ROYAL INSTITUTE OF TECHNOLOGY

The OSI model

Application layer



- Application protocols like
  - HTTP
  - FTP
  - SSH
- In power systems:
  - MMS (IEC 61850-8-2)
  - IEC 60870-5-104 (an RTU protocol over IP)
- More about this later…

ROYAL INSTITUTE OF TECHNOLOGY

The OSI model

Transport layer

Application
Transport
Network
Data Link
Physical

- Transport layer protocols include:
  - Transmission Control Protocol (streams)
  - User Datagram Protocol (datagrams)

Transport

- **TCP header fields**
  - Source/destination port
  - Sequence number
  - Acknowledgement (Ack) number
  - Window size
  - Checksum
  - Options

TCP Header

Bit offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Source port																Destination port															
32	Sequence number																															
64	Acknowledgment number																															
96	Data offset				Reserved				CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
128	Checksum																Urgent pointer															
160 ...	Options (if Data Offset > 5) ...																								padding							

ROYAL INSTITUTE OF TECHNOLOGY

The OSI model

Network layer

Application
Transport
Network
Data Link
Physical

- Routing of packets at this layer

  - A router forwards packets toward destination

  - Internet Protocol

    - **IP header fields**
      - Source/destination IP address
      - Time-to-live – prevents immortal lost packets
      - Unique ID
      - Checksum
      - Options

Network

bit offset	0–3	4–7	8–13	14-15	16–18	19–31
0	Version	Header Length	Differentiated Services Code Point	Explicit Congestion Notification	Total Length	
32	Identification				Flags	Fragment Offset
64	Time to Live		Protocol		Header Checksum	
96	Source IP Address					
128	Destination IP Address					
160	Options (if Header Length > 5)					
160 or 192+	Data					

ROYAL INSTITUTE OF TECHNOLOGY

The OSI model

Data Link layer

Application
Transport
Network
Data Link
Physical

Transfer data between adjacent nodes on a link

- Do not cross boundary of a local network

- Media Access Control (MAC)
- Logical Link Control (LLC)

Data Link

- **Ethernet frame header**
  - Preamble
  - Source/destination MAC address
  - Acknowledgement (Ack) number
  - Payload size
  - Cyclic redundancy check (CRC)
  - 12-octet interframe gap

802.3 Ethernet frame structure

Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype or length	Payload	Cyclic redundancy check	Interframe gap
7 octets of 10101010	1 octet of 10101011	6 octets	6 octets	(4 octets)	2 octets	46–1500 octets	4 octets	12 octets
		64–1522 octets						
72–1530 octets								
84–1542 octets								

ROYAL INSTITUTE OF TECHNOLOGY

The OSI model

Data Link layer – Media Access Control (MAC)

Application
Transport
Network
Data Link
Physical

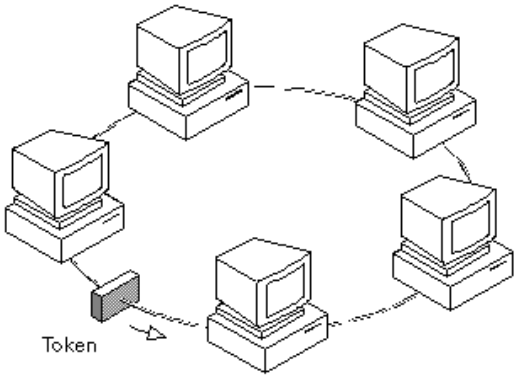
- Determines who gets access to the medium

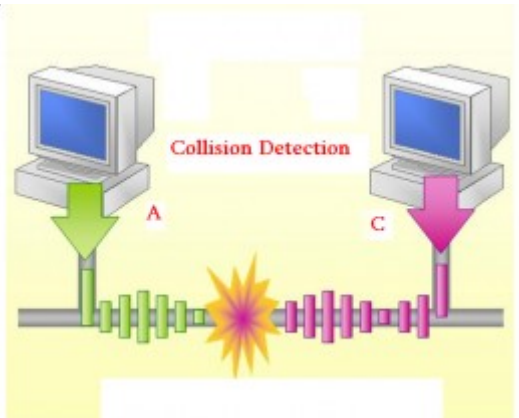
  - Token passing
    - Whoever **has the token** can send

  - Carrier Sense Multiple Access (CSMA)
    - **Listens** whether someone is sending

  - Collision Detection (CD)
    - Bits transmitted on the medium collide
    - Collision needs to be resolved

Data Link





ROYAL INSTITUTE OF TECHNOLOGY

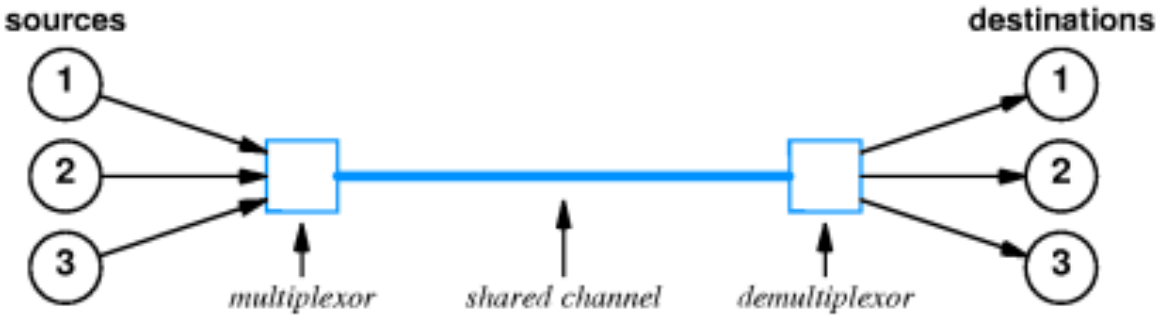
The OSI model

Data Link layer – Logical Link Control (LLC)

Application
Transport
Network
Data Link
Physical

- **Multiplexing** network layer packets
- Error handling in some link layer protocols

Data Link



ROYAL INSTITUTE OF TECHNOLOGY

The OSI model

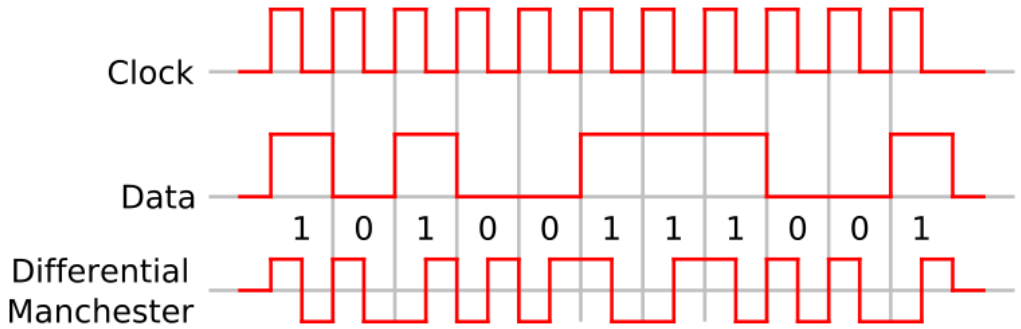
Physical layer

Application
Transport
Network
Data Link
Physical

- Bit-by-bit delivery

- Specifies
  - Medium - Cable/Fibre/Radio
    - Connector types
    - Cable length
  - Signal characteristics
    - Voltage
    - Frequency of carrier signal
    - Impedence
  - Line coding
    - Tuned for physical channel
    - For modulation
  - Signalling
    - Start/stop

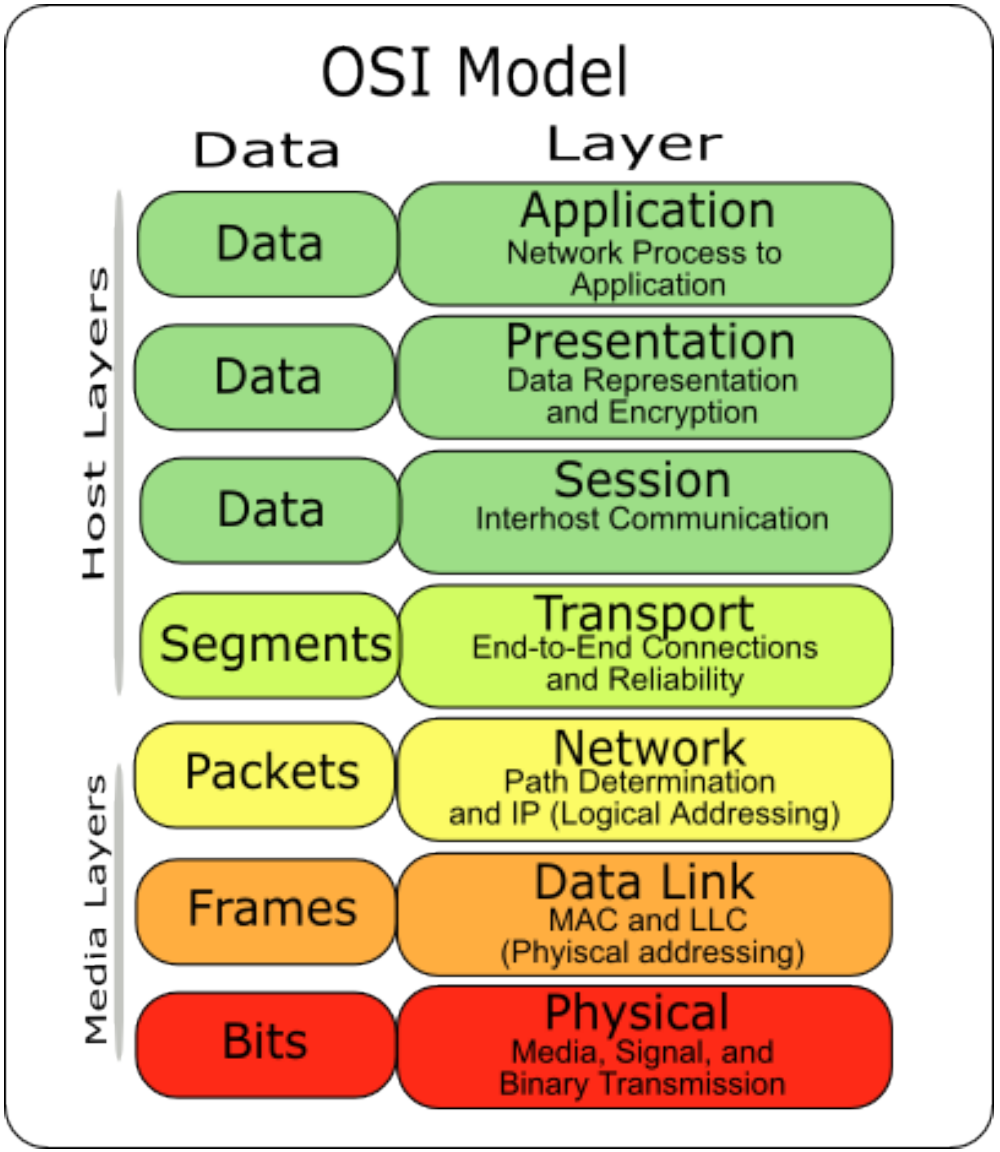
Physical



ROYAL INSTITUTE OF TECHNOLOGY

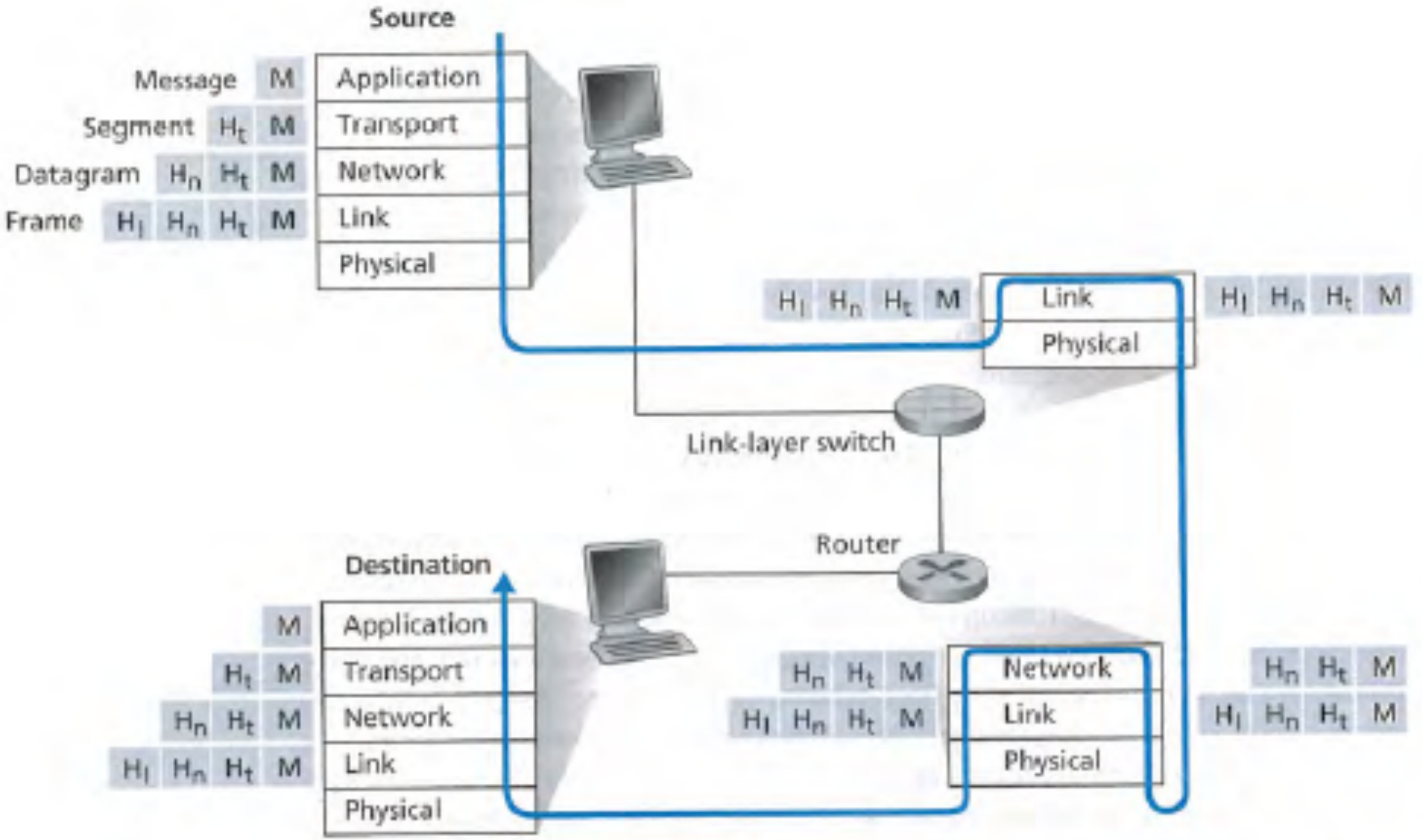
The OSI model

Application
Transport
Network
Data Link
Physical



The OSI model

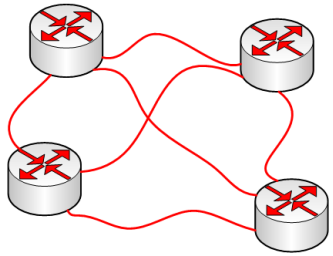
Application
Transport
Network
Data Link



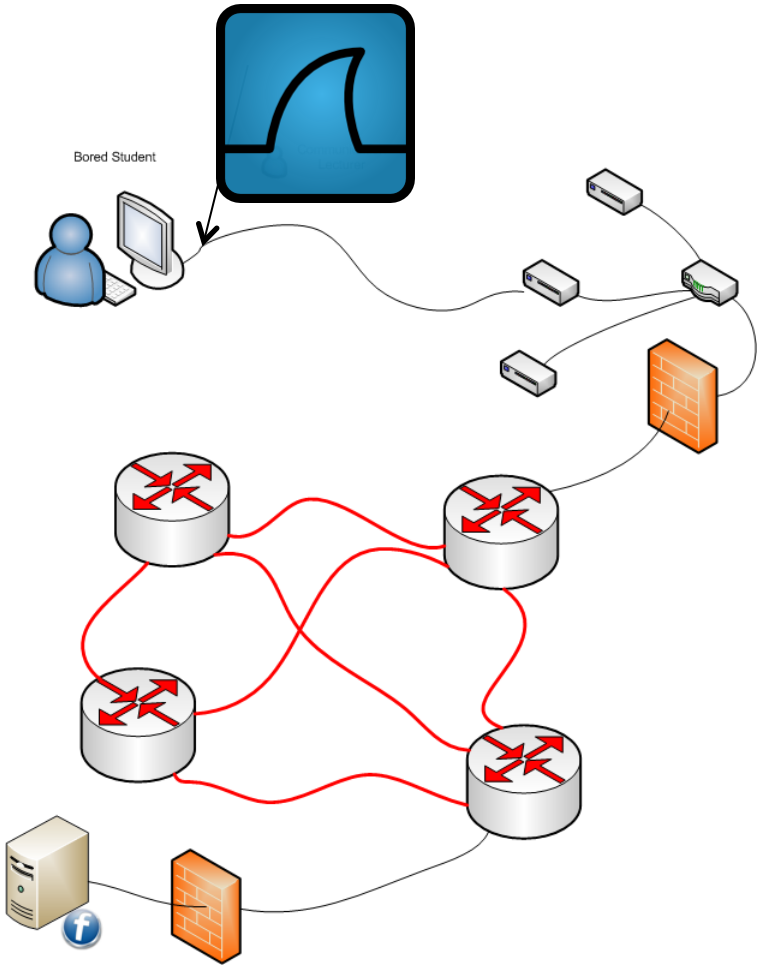
ROYAL INSTITUTE OF TECHNOLOGY

Communication Networks

Wireshark



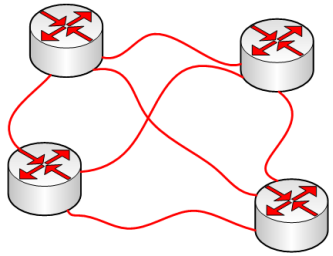
- Example using Wireshark:
  - Set Wireshark filter to only capture HTTP
  - Start the recording
  - Request the service (a website in this case)
  - Watch the capture
  - Stop the capture when complete
  - Analyse the results



ROYAL INSTITUTE OF TECHNOLOGY

Communication Networks

DNS protocol - example



(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
366	11.767290	192.168.0.31	192.168.0.28	SNMP	get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.7.1
367	11.768865	192.168.0.28	192.168.0.31	SNMP	get-request SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1.
369	11.775952	192.168.0.31	192.168.0.28	SNMP	get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1
381	12.286091	192.168.0.28	192.168.0.1	DNS	Standard query A www.cnn.com
384	12.311862	192.168.0.1	192.168.0.28	DNS	Standard query response A 64.236.91.21 A 64.236.91.23 A 64.23
385	12.312727	192.168.0.28	64.236.91.21	TCP	56606 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
386	12.361495	64.236.91.21	192.168.0.28	TCP	http > 56606 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
387	12.361583	192.168.0.28	64.236.91.21	TCP	56606 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
388	12.361805	192.168.0.28	64.236.91.21	HTTP	GET / HTTP/1.1
389	12.413166	64.236.91.21	192.168.0.28	TCP	http > 56606 [ACK] Seq=1 Ack=845 Win=6960 Len=0
390	12.413611	64.236.91.21	192.168.0.28	TCP	[TCP segment of a reassembled PDU]
391	12.414386	64.236.91.21	192.168.0.28	TCP	[TCP segment of a reassembled PDU]

```
⊞ Frame 384 (167 bytes on wire, 167 bytes captured)
⊞ Ethernet II, Src: Sparklan_04:d0:9e (00:0e:8e:04:d0:9e), Dst: HonHaiPr_26:66:a2 (00:1c:26:26:66:a2)
⊞ Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.28 (192.168.0.28)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 62872 (62872)
⊟ Domain Name System (response)
    [Request In: 381]
    [Time: 0.025771000 seconds]
    Transaction ID: 0xcf1f
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.cnn.com: type A, class IN
        Name: www.cnn.com
        Type: A (Host address)
        Class: IN (0x0001)
  ⊟ Answers
    ⊞ www.cnn.com: type A, class IN, addr 64.236.91.21
```

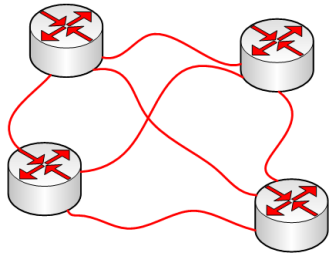
```
0000  00 1c 26 26 66 a2 00 0e  8e 04 d0 9e 08 00 45 00   ..&&f... ......E.
0010  00 99 00 00 40 00 40 11  b8 e6 c0 a8 00 01 c0 a8   ....@.@. ........
0020  00 1c 00 35 f5 98 00 85  98 5a cf 1f 81 80 00 01   ...5.... .Z......
0030  00 06 00 00 00 00 03 77  77 77 03 63 6e 6e 03 63   .......w ww.cnn.c
0040  6f 6d 00 00 01 00 01 c0  0c 00 01 00 01 00 00 00   om...... ........
0050  b7 00 04 40 ec 5b 15 c0  0c 00 01 00 01 00 00 00   ...@.[.. ........
0060  b7 00 04 40 ec 5b 17 c0  0c 00 01 00 01 00 00 00   ...@.[.. ........
0070  b7 00 04 40 ec 10 14 c0  0c 00 01 00 01 00 00 00   ...@.... ........
```

This is a response to the DNS query in this fr... | Packets: 1273 Displayed: 909 Marked: 0 Dropped: 0 | Profile: Default

ROYAL INSTITUTE OF TECHNOLOGY

Communication Networks

Wireshark

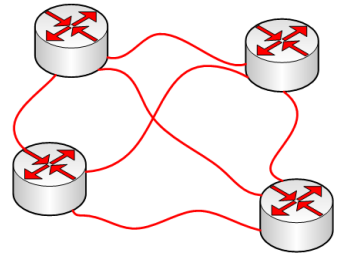


```
⊞ Frame 384 (167 bytes on wire, 167 bytes captured)
⊞ Ethernet II, Src: Sparklan_04:d0:9e (00:0e:8e:04:d0:9e)
⊞ Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst:
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port
⊟ Domain Name System (response)
    [Request In: 381]
    [Time: 0.025771000 seconds]
    Transaction ID: 0xcf1f
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.cnn.com: type A, class IN
        Name: www.cnn.com
        Type: A (Host address)
        Class: IN (0x0001)
  ⊟ Answers
    ⊞ www.cnn.com: type A, class IN, addr 64.236.91.21
```

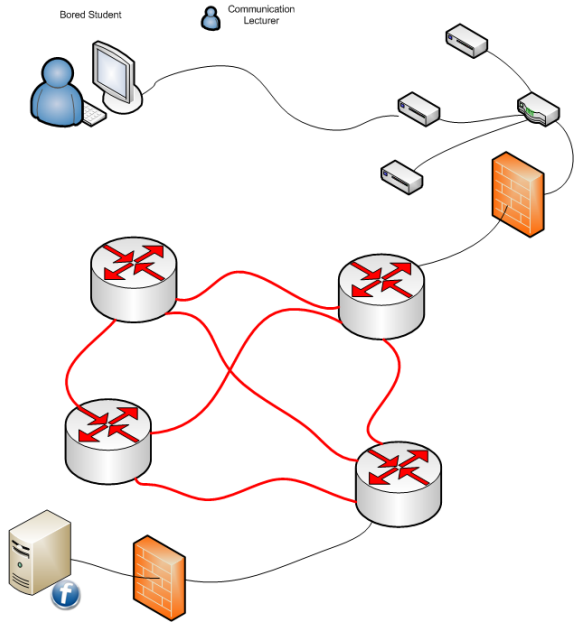
ROYAL INSTITUTE OF TECHNOLOGY

Protocol Basics

Some observations from the HTTP protocol example

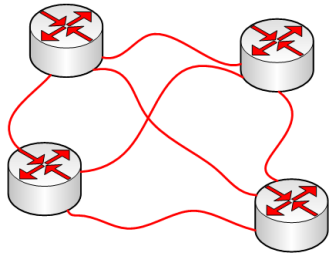


- Some observations:
  - Often need multiple services to access the desired service eg. DNS translates hostname in URL to IP-address and HTTP is used to fetch the webpage data
  - There appear to be layers in the protocols
  - Some of the layers are common even when different application-layer services are used eg. Ethernet, IP…
  - There are some containers used:
    - Datagram
    - Packet
    - Frame
  - Identification of host, service, source, destination:
    - MAC `00:0e:8e:04…`
    - IP `192.168.0.1`
    - Port `80 (HTTP)`



ROYAL INSTITUTE OF TECHNOLOGY

Circuit and Packet Switching

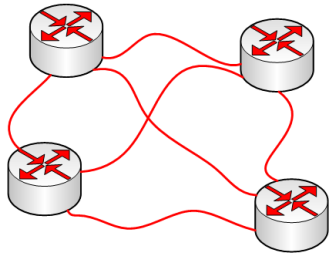


- Circuit switching
- Packet switching

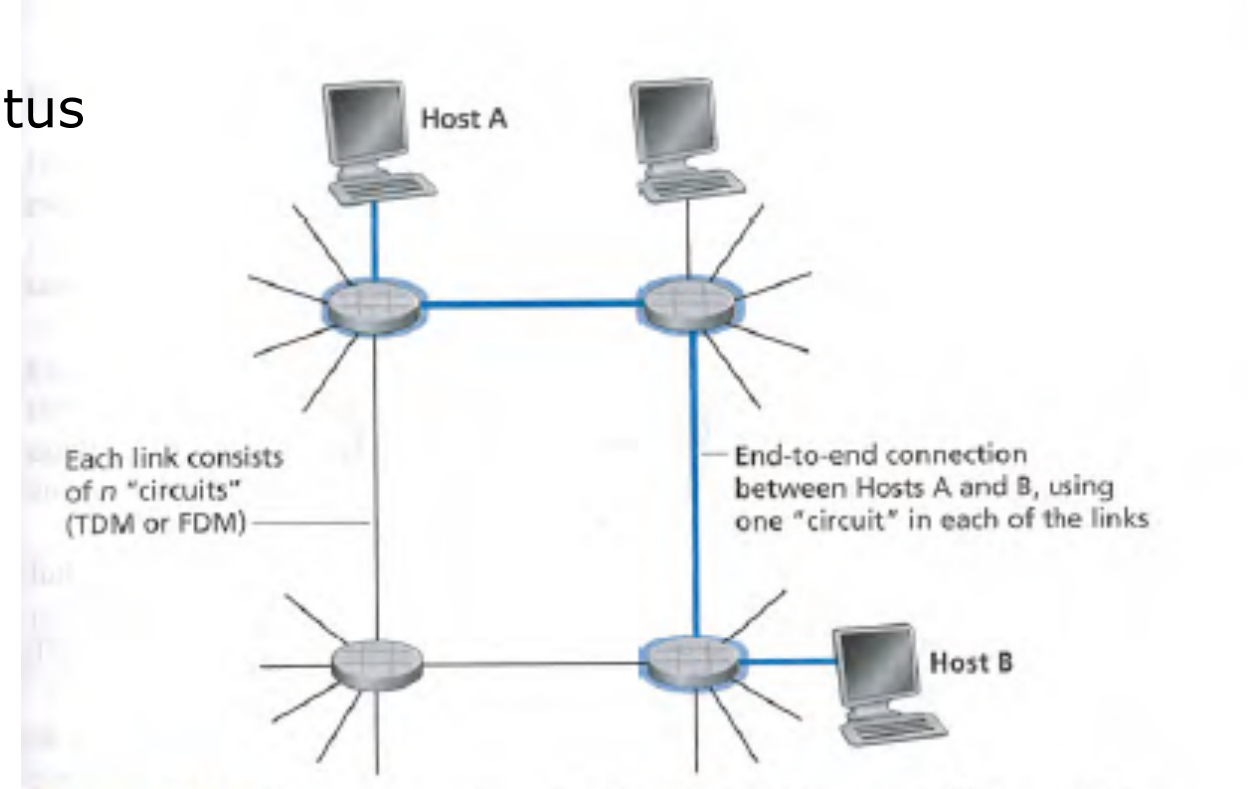
ROYAL INSTITUTE OF TECHNOLOGY

Circuit and Packet Switching

Circuit Switching

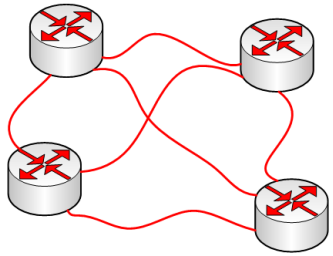


- Like an old telephone network
- Fixed connection
  - Follows same route
  - Routers need to maintain status
- Handshake required
  - TCP does this
- Allows for host flow control
- **Reliable delivery**



Circuit and Packet Switching

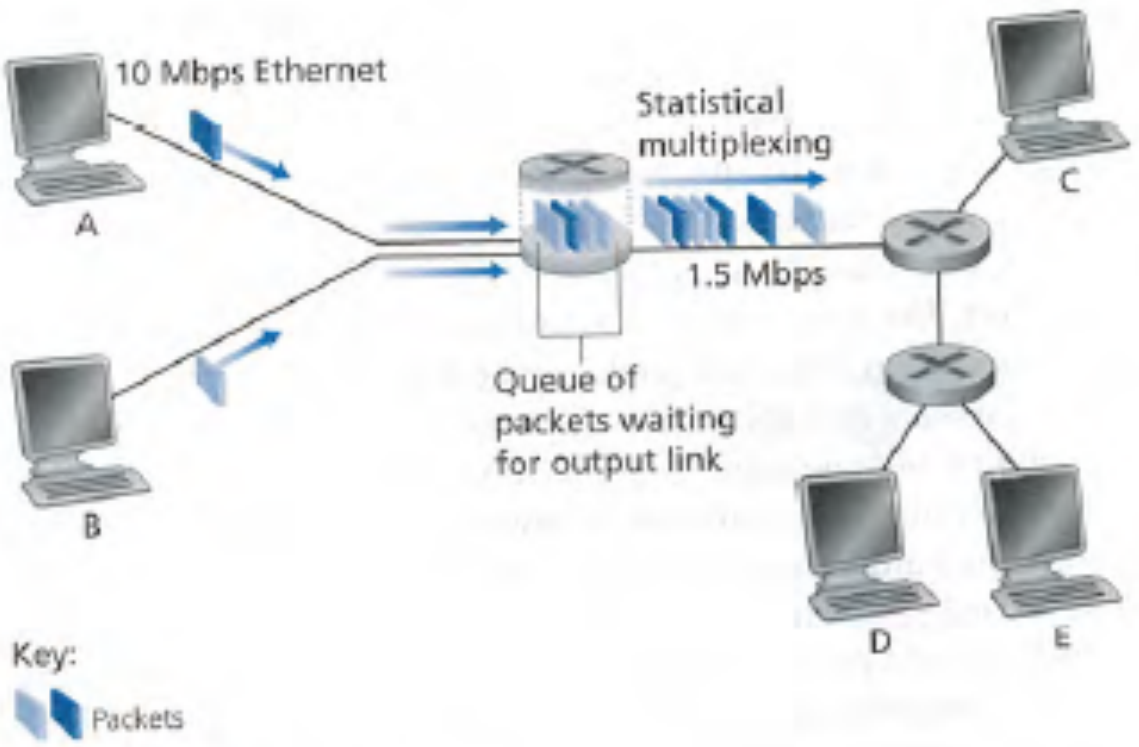
Packet Switching



- Like the postal service

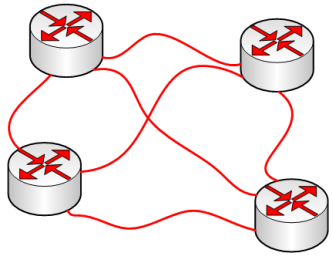
- No connections
  - Follows stochastic route
  - Stateless routers

  - IP is packet switched
  - Most link-layer protocols



ROYAL INSTITUTE OF TECHNOLOGY

Circuit and Packet Switching

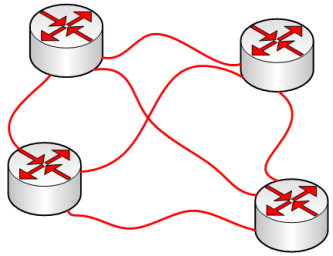


- Circuit switching
- Packet switching

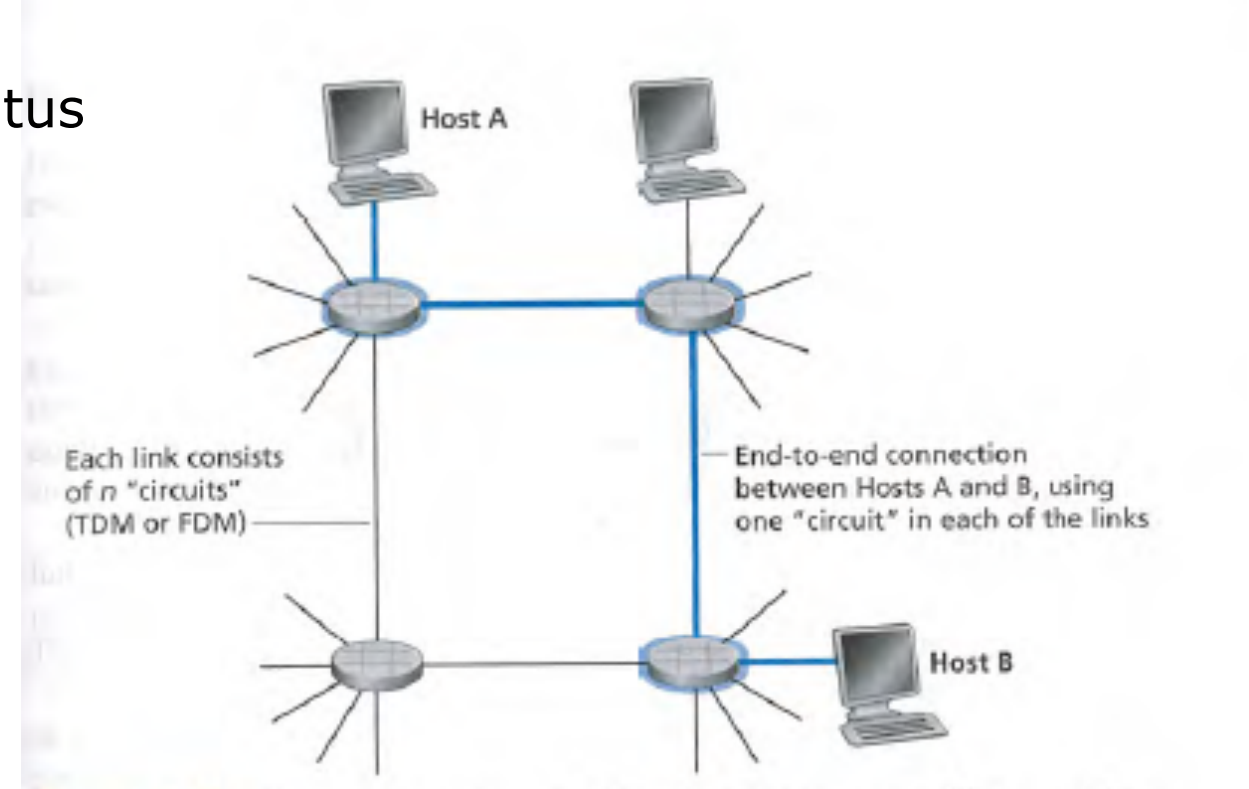
ROYAL INSTITUTE OF TECHNOLOGY

Circuit and Packet Switching

Circuit Switching

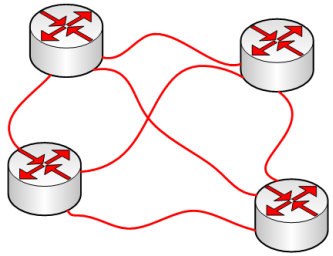


- Like an old telephone network
- Fixed connection
  - Follows same route
  - Routers need to maintain status
- Handshake required
  - TCP does this
- Allows for host flow control
- **Reliable delivery**



Circuit and Packet Switching

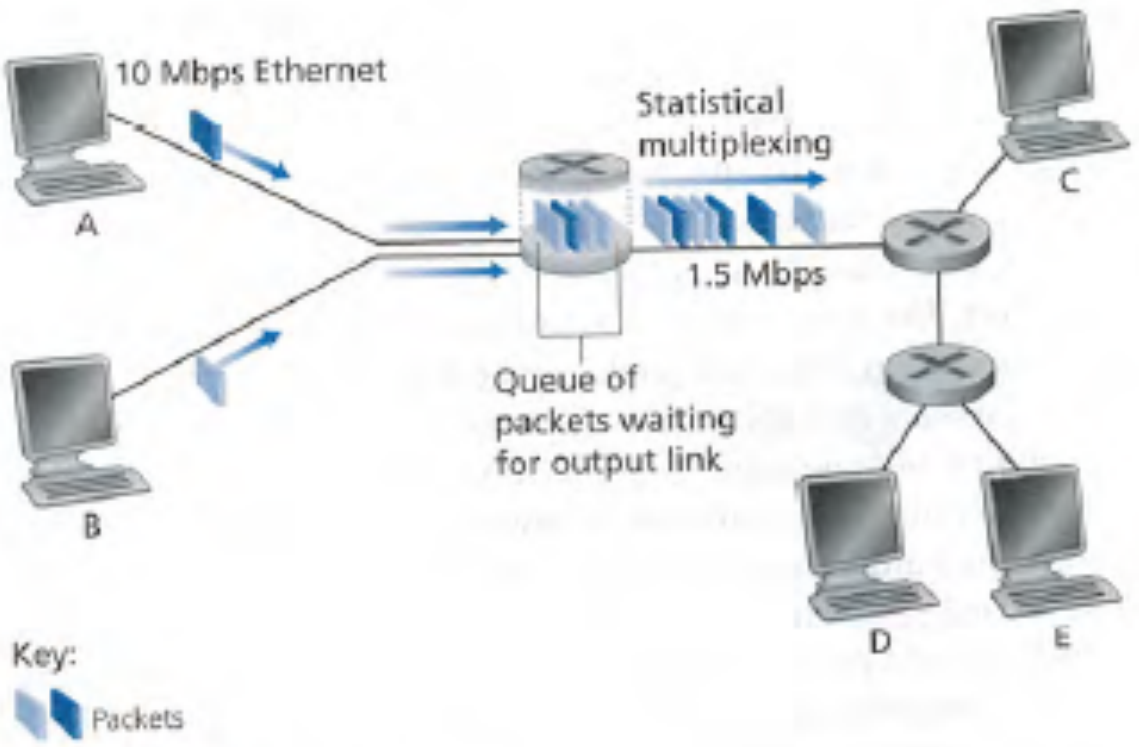
Packet Switching



- Like the postal service

- No connections
  - Follows stochastic route
  - Stateless routers

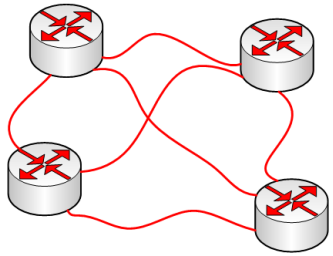
  - IP is packet switched
  - Most link-layer protocols

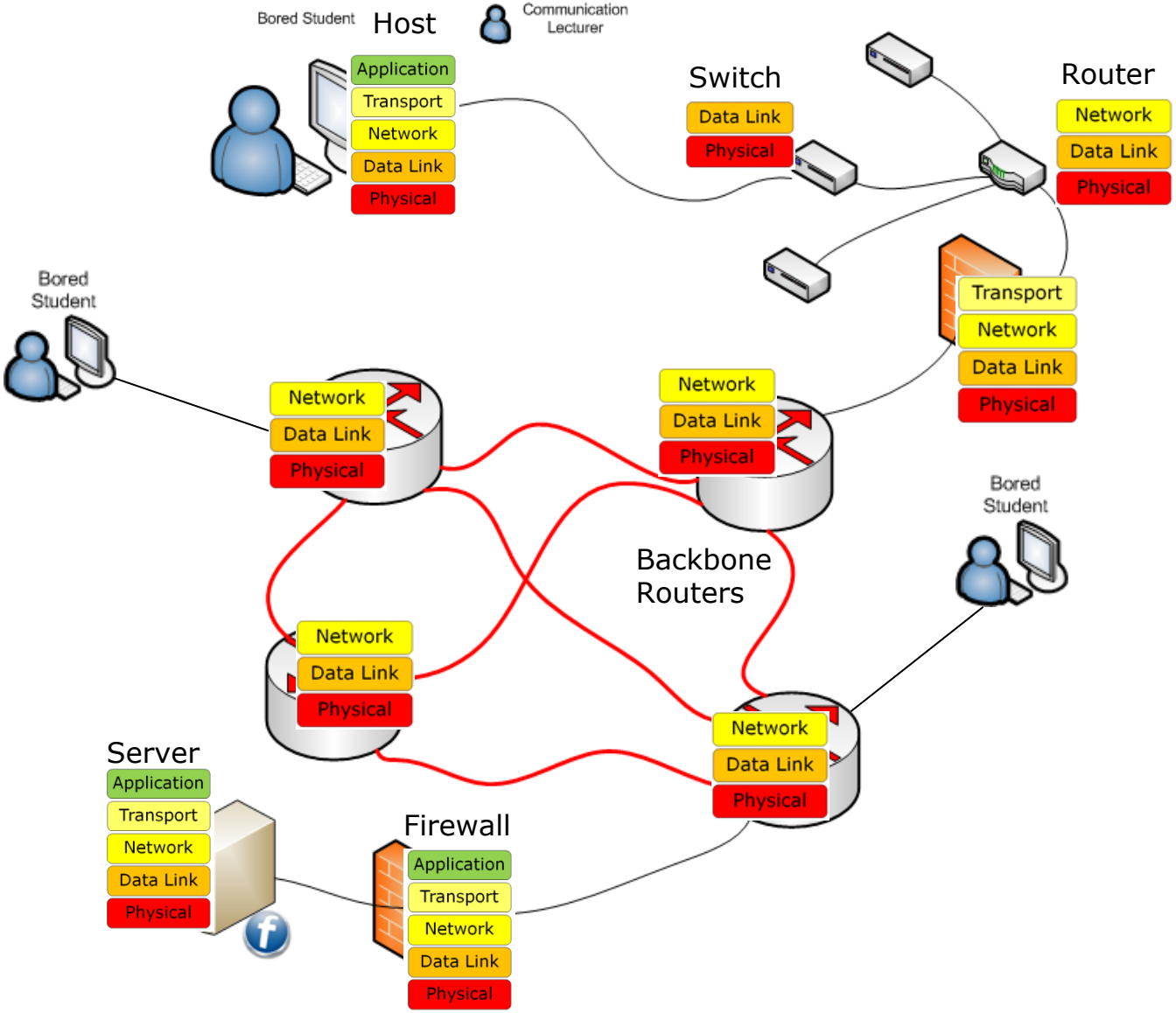


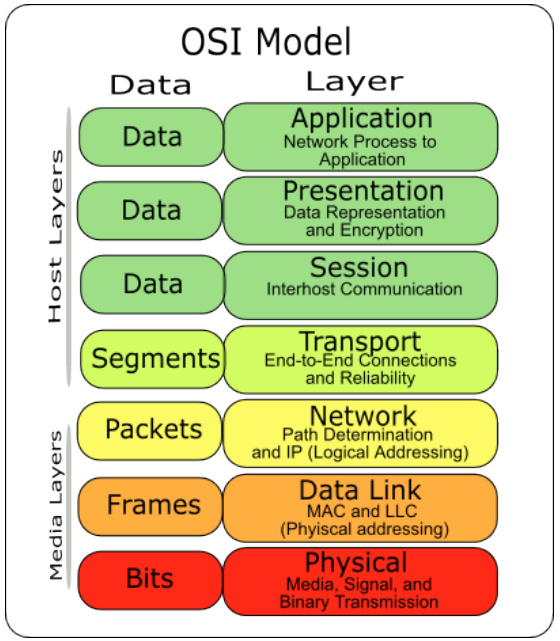
ROYAL INSTITUTE OF TECHNOLOGY

Communication Networks

Recap of example



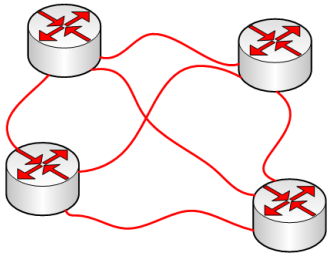


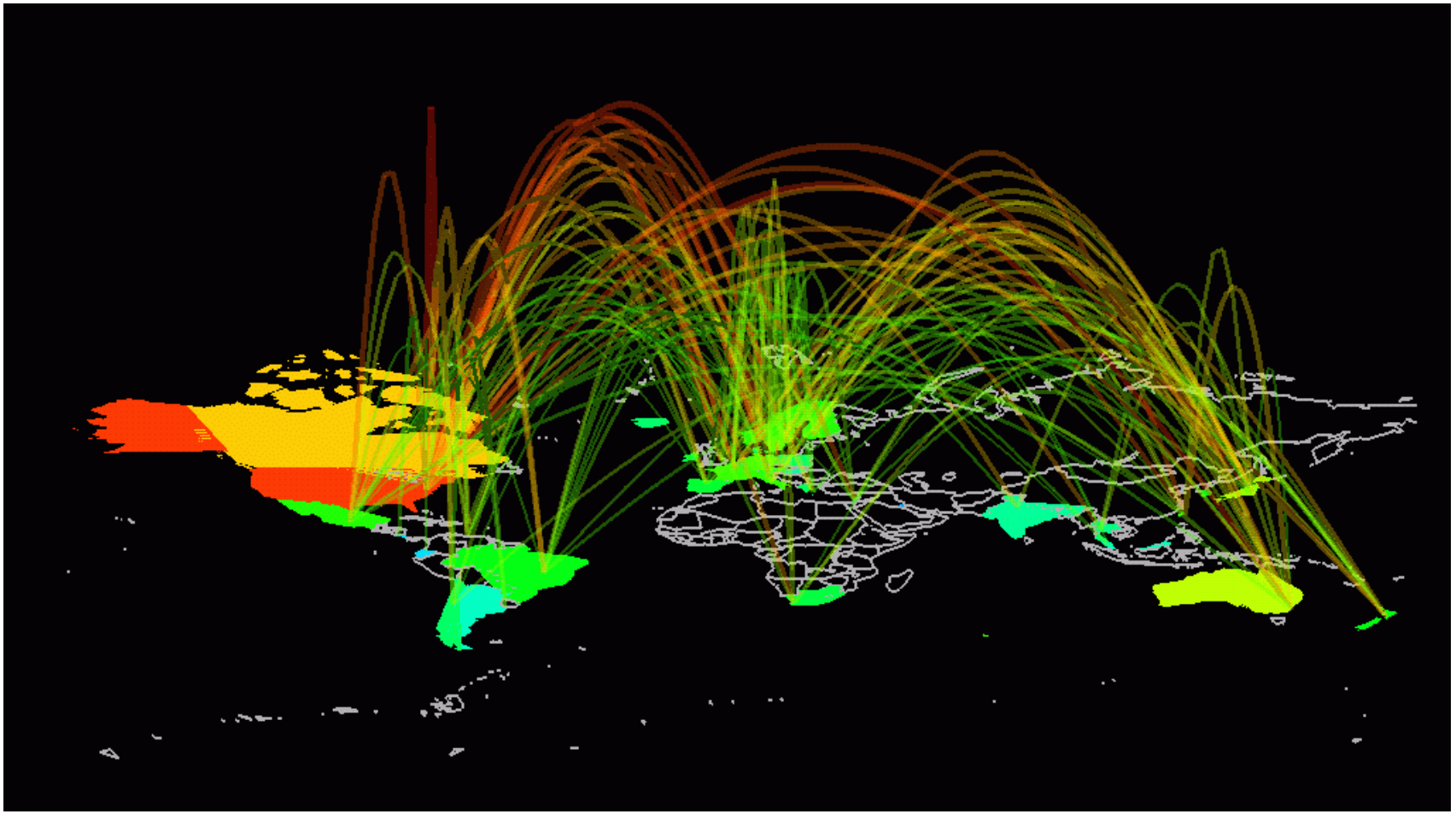


ROYAL INSTITUTE OF TECHNOLOGY

Brief distraction

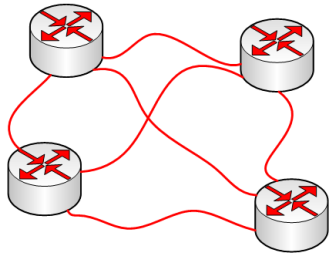
Internet backbone networks





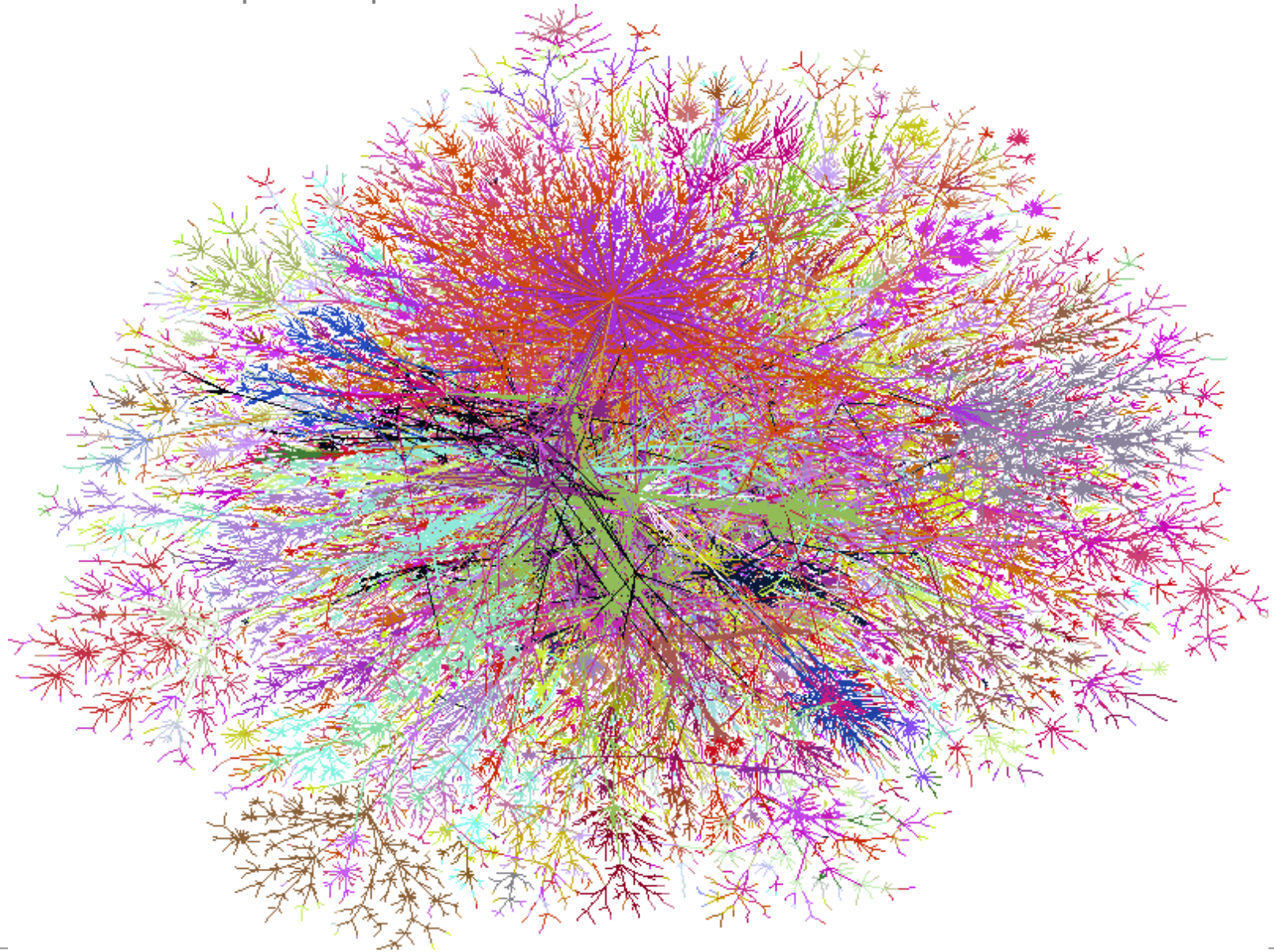
Map from Bell Labs

ROYAL INSTITUTE OF TECHNOLOGY



Brief distraction

Internet splat map



ROYAL INSTITUTE OF TECHNOLOGY

Physical media and devices

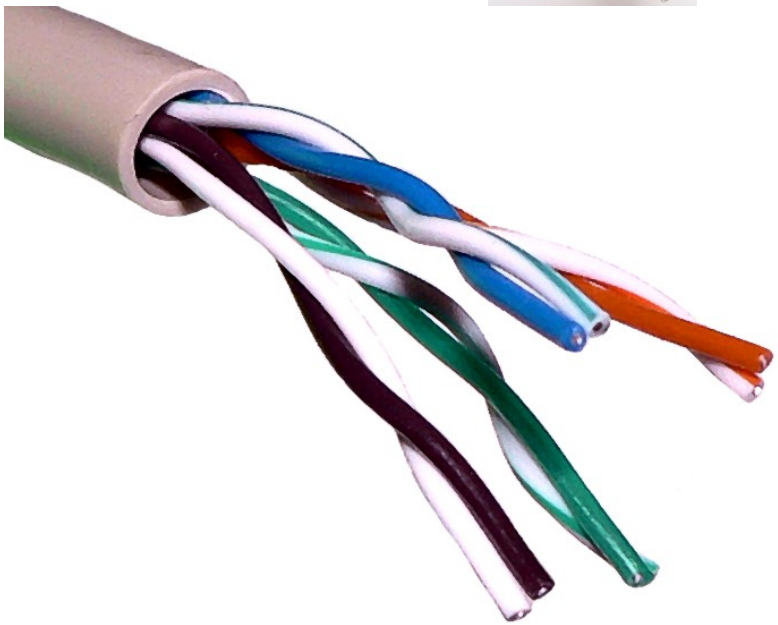
- Twisted-Pair Copper wire
- Coaxial Cable
- Fiber Optics
- Terrestrial Radio
- Satellite Radio
- Communication devices

Physical

ROYAL INSTITUTE OF TECHNOLOGY

Physical media

Twisted-pair copper wire

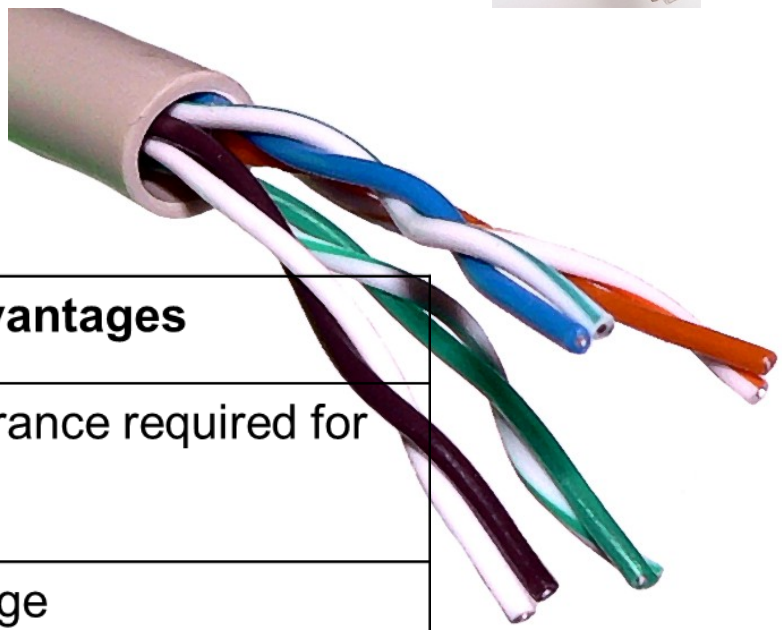


- Used in 99% of connections
- 10*BASE-T Ethernet standard
  - Uses RJ45 connector
- Cat 5 Unshielded twisted pair
  - Speeds up to 1Gbps
- Digital Subscriber Line (DSL)
  - Speeds around 10Mbps

ROYAL INSTITUTE OF TECHNOLOGY

Physical media

Twisted-pair copper wire

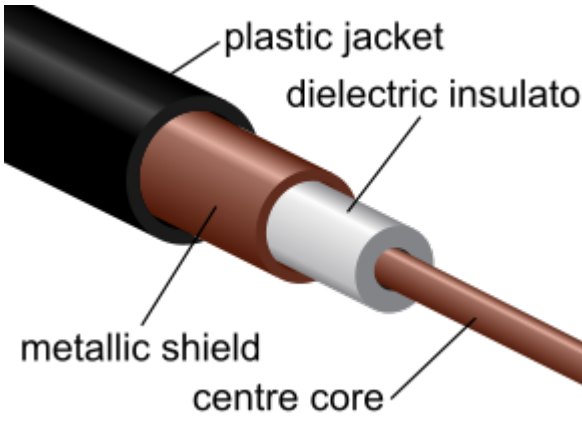


Advantages	Disadvantages
No Licensing, Fewer approvals	Right-of way clearance required for buried cable
Existing pole infrastructure	Subject to breakage
Economical for short distances	Subject to water ingress
Relatively high channel capacity (up to 1.54 MHz) for short distances	Subject to ground potential rise due to power faults and lightning
	Failures may be difficult to pinpoint
	Inflexible network configuration

ROYAL INSTITUTE OF TECHNOLOGY

Physical media

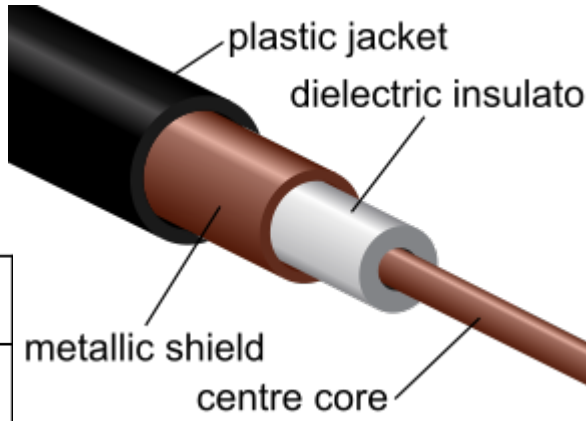
Coaxial cable



- Used in older Ethernet standards
  - 10BASE5
  - 10BASE2
- Common in cable TV installations
  - Cable modems up to 24Mbps
- Frequency multiplexing
  - Shared medium

Physical media

Coaxial cable

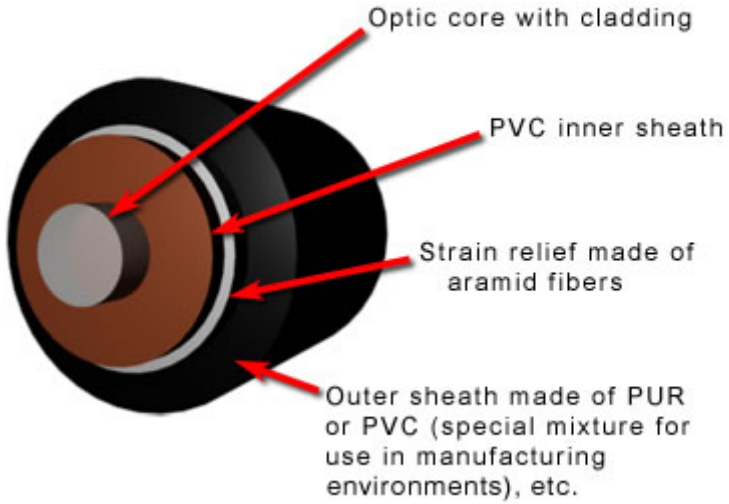


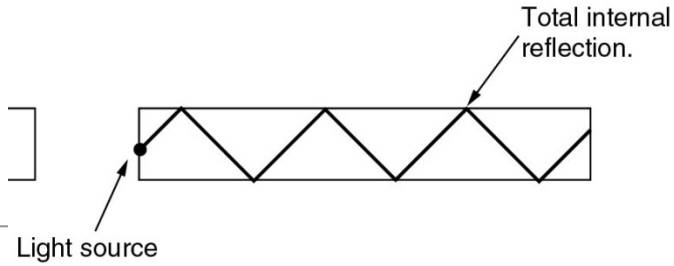
Advantages	Disadvantages
No Licensing, Fewer approvals	Right-of way clearance required for buried cable
Existing pole infrastructure	Subject to breakage
Economical for short distances	Subject to water ingress
Relatively high channel capacity than Twisted Pair Metallic	Subject to ground potential rise due to power faults and lightning
More immune to RF noise interference than Twisted Pair Metallic	Failures may be difficult to pinpoint
	Inflexible network configuration

Physical media

Fiber optics

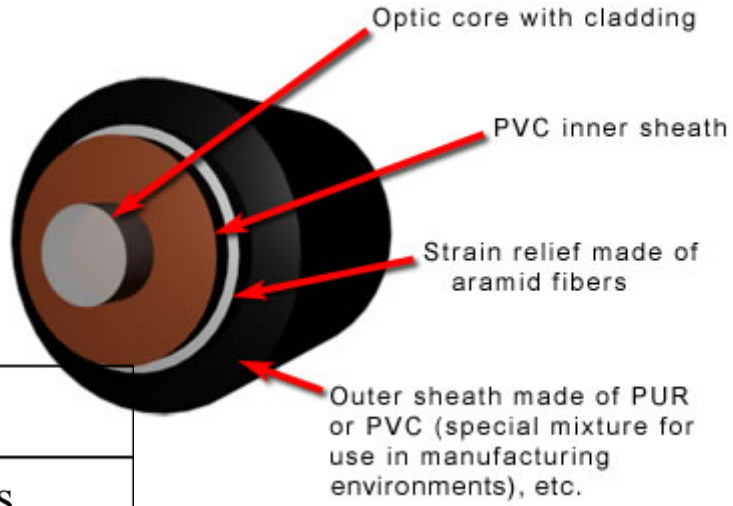
- Often many cores in a single cable
- Very low attenuation up to 100km
- Used for undersea cables
- Very high speeds
  - 100GBASE-ER4 (100Gbps 40km)



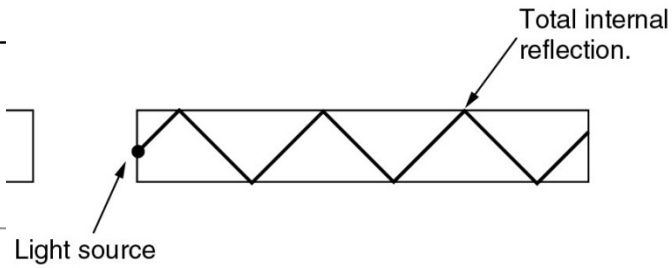


Physical media

Fiber optics



Advantages	Disadvantages
Immune to electromagnetic interference	Novel technology, i.e. new skills must be learned
Immune to ground potential rise	Expensive test equipment
High channel capacity	Inflexible network configuration
Low operating cost	Cable subject to breakage and water ingress
No licensing required	Failures may be difficult to pinpoint



ROYAL INSTITUTE OF TECHNOLOGY

Physical media

Terrestrial radio

- Two main variants
  - Local-area unidirectional
  - Long-distance point-to-point

  - Wireless LAN
    - IEEE 802.11*x*

  - Point-to-point microwave

ROYAL INSTITUTE OF TECHNOLOGY

Physical media

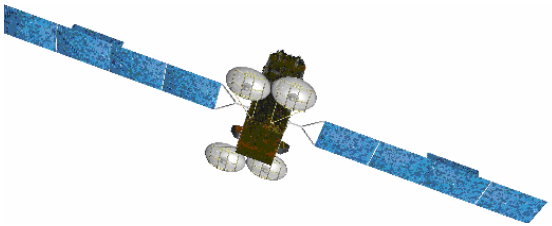
Terrestrial radio

Advantages	Disadvantages
Wide Area Coverage	Total dependency on a remote facility
Easy access to remote sites	Less control over transmission
Costs independent of distance	Transmission time delay
Low error rates	Reduced transmission during solar equinox
Adaptable to changing network patterns	Continual leasing cost
No right-of-way necessary, earth stations located at premises	

ROYAL INSTITUTE OF TECHNOLOGY

Physical media

Satellite radio



- Usually used in
  - Telephone networks
  - Internet backbone links

  - Long propagation delay
    - 36,000 km trip one-way
    - 280 ms delay

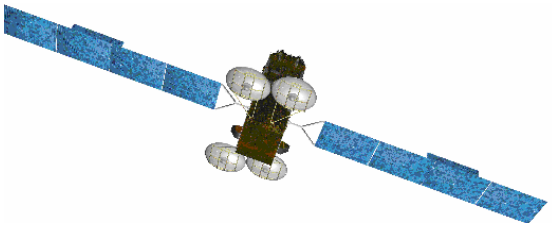
  - Used for high-speed internet where no infrastructure exists

- Geostationary
- Low-earth orbit

ROYAL INSTITUTE OF TECHNOLOGY

Physical media

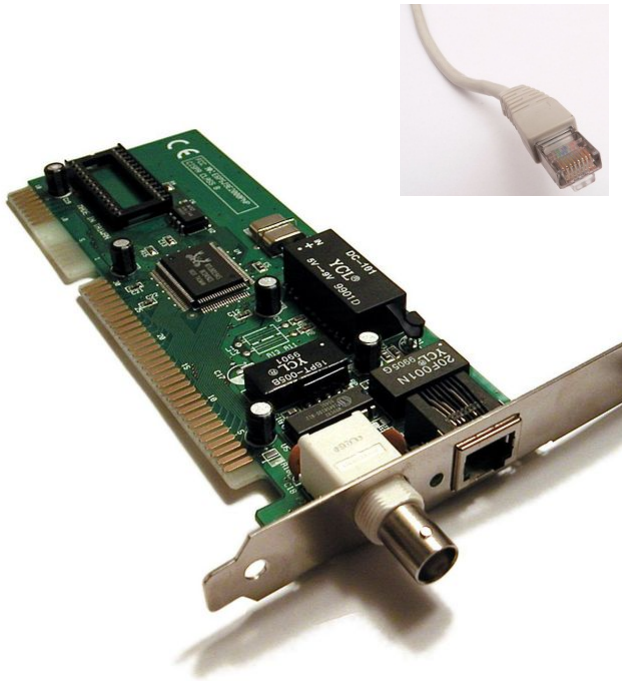
Satellite radio



Advantages	Disadvantages
Wide Area Coverage	Total dependency on a remote facility
Easy access to remote sites	Less control over transmission
Costs independent of distance	Transmission time delay
Low error rates	Reduced transmission during solar equinox
Adaptable to changing network patterns	Continual leasing cost
No right-of-way necessary, earth stations located at premises	

Physical media

Communication devices



- Network Interface Controller (NIC)

  - Physical and data link layer
  - Sometimes even network layer

  - Ethernet cards have unique MAC address

  - Interface to host computer
    - Polling
    - Interrupt-driven
    - Direct Memory Access

ROYAL INSTITUTE OF TECHNOLOGY

Physical media

Communication devices

- Hub/Repeater
  - Physical layer only
  - Usually with UTP or fiber
  - Extend range – point-to-point
  - Create multi-point segment

Physical

ROYAL INSTITUTE OF TECHNOLOGY

Physical media

Communication devices

- Switch
  - Physical and data link layers (bridge)
  - Managed switches exist
    - Security
    - Performance
  - Learns the MAC address of each connected device
  - "Switch" methods
    - Store-and-forward
    - Cut-through
    - Fragment-free – first 64 bytes
    - Adaptive – choose between the 3 above

Physical media

Communication devices

- Router

  - Operates at the network layer

  - Traffic directing

  - Routing table – example “route PRINT”
    - Directs packet to next network

  - SoHo devices – cheap, simple
  - Core routers
    - High-speed connections
    - Performance management/tuning tools

ROYAL INSTITUTE OF TECHNOLOGY

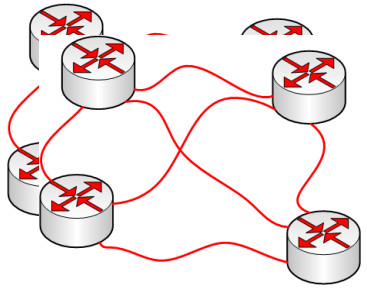
Physical media

Communication devices

- Modem
  - Modulator/Demodulator
  - Modulates digital bitstream into analog signal
  - Most commonly used for phone line internet
  - Radio
    - 3G, GPRS
    - Satellite
  - Cable TV

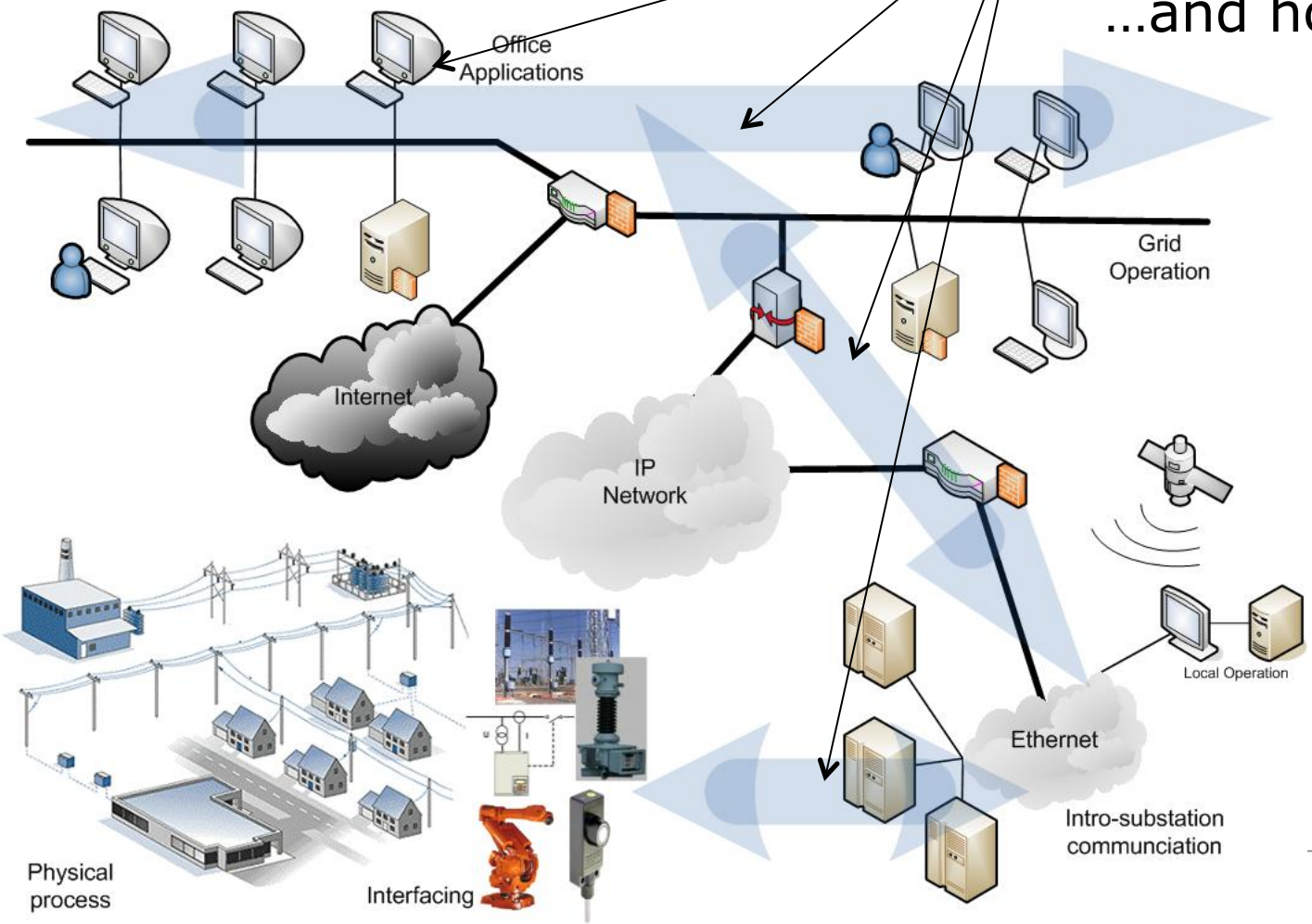
What to expect next…

Protocols used in SCADA and SAS



Which protocols are used?

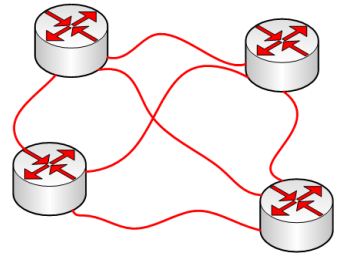
…and how do they work?



ROYAL INSTITUTE OF TECHNOLOGY

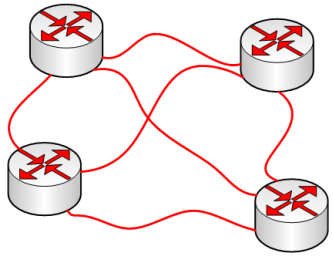
Communication Networks

Conclusion



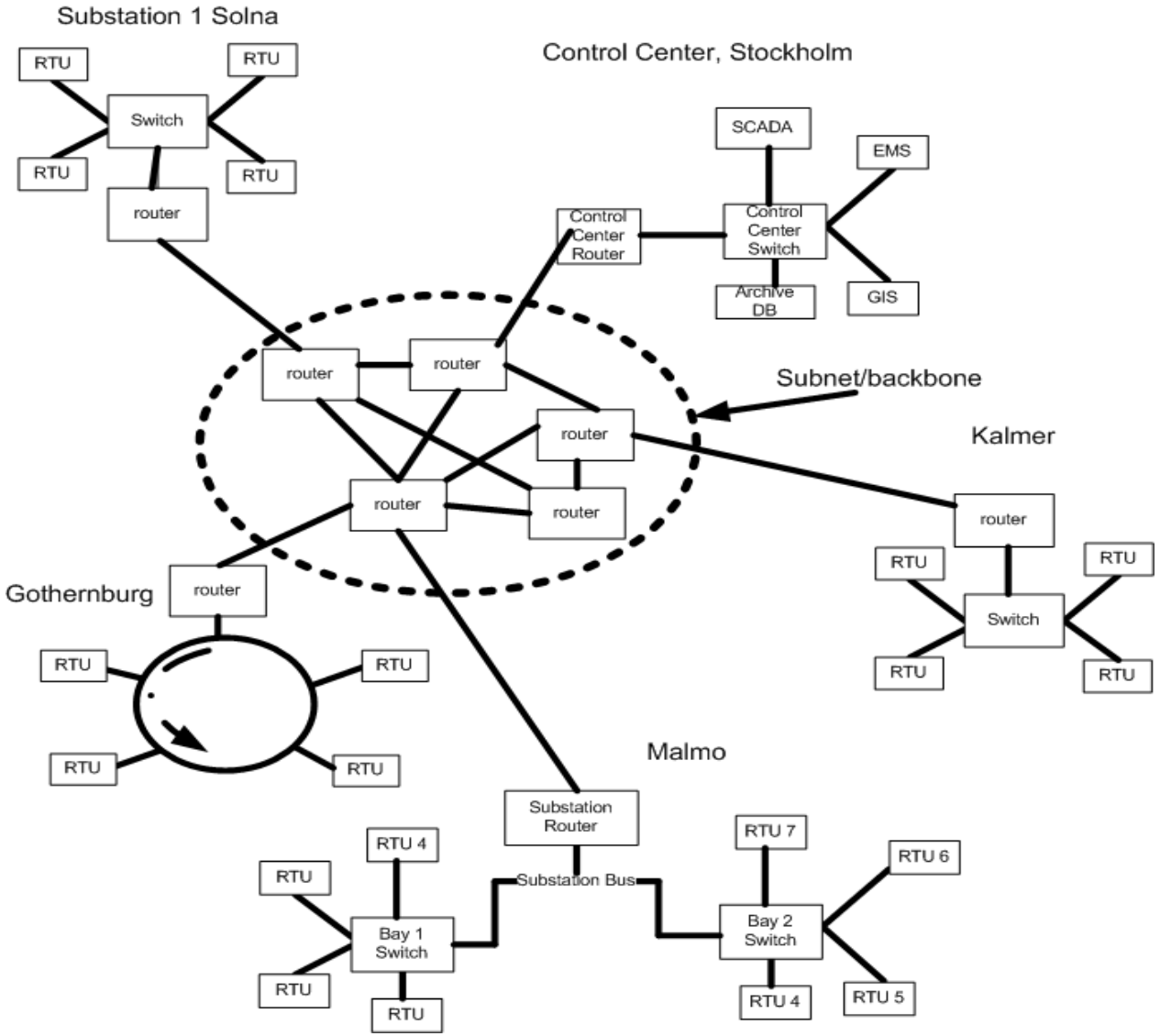
- We can view networks in terms of the OSI layered model
- The lowest 3 layers provide the infrastructure for transmitting and delivering messages
- The higher layers implement the host-based application-specific communication
- A combination of protocols can be used to provides services eg. DNS lookup before sending HTTP GET
- Now we can say a lot more about the process and station bus
- We have looked at some common physical media solutions
- Common communication infrastructure devices

ROYAL INSTITUTE OF TECHNOLOGY



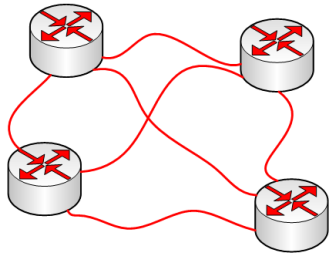
What to expect next…

Topology of a network



ROYAL INSTITUTE OF TECHNOLOGY

What to expect next…



- Topology of a network
- Media Access Control Techniques
- Routing and addressing
- Protocols found in SCADA and SAS